AX1200S 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. 1.4 対応

AX12S-S001-A0

AlaxalA

■対象製品

このマニュアルは AX1200S モデルを対象に記載しています。また，AX1200S のソフトウェア Ver. 1.4 の機能について記載しています。ソフトウェア機能は，ソフトウェア OS-LT によってサポートする機能について記載します。

■輸出時の注意

本製品を輸出される場合には，外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上，必要な手続きをお取りください。
なお，ご不明な場合は，弊社担当営業にお問い合わせください。

■商標一覧

Ethernet は，米国 Xerox Corp. の商品名称です。
Microsoft は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
Windows は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
イーサネットは，富士ゼロックス（株）の商品名称です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■マニュアルはよく読み，保管してください。

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

■ご注意

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

■発行

２０１０年　3月 （第１１版） ＡＸ １２ Ｓ － Ｓ ００１ － Ａ ０

■著作権

変更履歴

【Ver. 1.4（第 11 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
3　収容条件	•「(11) レイヤ 2 認証の注記を変更しました。
4　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。
9　装置の管理	• system l2-table mode コマンドを追加しました。 •「イベントトレースのモニタ表示実施と停止」の記述を変更しました。 •「イベントトレース・装置障害ログ情報の確認」の記述を変更しました。
11　イーサネット	•「メディアタイプ設定時の注意事項」の記述を変更しました。
12　リンクアグリゲーション	• スタンバイリンク機能の「(4) リンクダウンモード使用時の注意事項」の記述を変更しました。
14　MAC アドレス学習	• 注意事項にレイヤ 2 認証機能使用時のエージング時間について記述を追加しました。
16　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，認証前中継を使用時の注意事項を追加しました。
20　IGMP snooping/MLD snooping の設定と運用	• MLD Query メッセージ送信元 IP アドレスの設定の注意事項を変更しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 1.4（第 10 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
収容条件	•「(11) レイヤ 2 認証機能」に認証専用 IPv4 アクセスリストの収容条件を追加しました。また，IEEE802.1X・Web 認証・MAC 認証の最大端末数表の記述を変更しました。
RADIUS を使用した認証	•「(3)RADIUS サーバへの復旧」に RADIUS サーバでの認証失敗時のカレントサーバについて説明文を追加しました。
装置情報のバックアップ・リストア	• 本項を追加しました。
リンクアグリゲーション使用時の注意事項	•「(4) チャネルグループ内のポートに障害が発生したとき」の記述を追加しました。
スタンバイリンク機能	•「(3) スタンバイリンクのモードについて」の記述を変更しました。 •「(4) リンクダウンモード使用時の注意事項」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. 1.4（第 9 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
収容条件	• 「(11) レイヤ 2 認証機能」にダイナミック VLAN モードの記述を追加し，従来のダイナミック VLAN モードをレガシーモードに変更しました。 （IEEE802.1X にはポート単位認証（動的）を追加）
システムファンクションリソース配分の設定	• 拡張認証機能の記述を変更しました。
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の関連コマンド一覧に，dot1x force-authorized，dot1x force-authorized vlan コマンドを追加しました。
レイヤ 2 認証機能との連携について	• ダイナミック VLAN モードの記述を追加し，従来のダイナミック VLAN モードをレガシーモードに変更しました。また，IEEE802.1X にポート単位認証（動的）を追加しました。
DHCP snooping	• 記載内容を全面変更しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 1.3（第 8 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
収容条件	• 「(2)MAC アドレステーブル」に注記を追加しました。 • 「(3)VLAN」の「(b)MAC VLAN」に注記を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 1.3（第 7 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
収容条件	• 「(3)VLAN」に「(a) プロトコル VLAN」を追加しました。 • 「(15)L2 ループ検知」を追加しました。
1000BASE-X 使用時の注意事項	• 「(3)1000BASE-BX の SFP 挿入時の注意事項」を追加しました。
レイヤ 2 スイッチ機能と他機能の共存について	• プロトコル VLAN サポートに伴い記述を変更しました。レイヤ 2 認証機能については，本項から削除しコンフィグレーションガイド Vol.2 参照としました。
プロトコル VLAN の解説	• 本項を追加しました。
プロトコル VLAN のコンフィグレーション	• 本項を追加しました。
レイヤ 2 認証機能との連携について	• MAC VLAN とレイヤ 2 認証機能について記述を変更しました。
MAC ポートのオプション機能	• レイヤ 2 認証機能と併用時の記述を変更しました。
ループガード	• 本項を追加しました。
ルートガード	• 本項を追加しました。
ループガードの設定	• 本項を追加しました。
ルートガードの設定	• 本項を追加しました。

章・節・項・タイトル	追加・変更内容
バインディングデータベース	•「(2) バインディングデータベースの保存」を追加しました。 •「(3) 保存したバインディングデータベースの復元」を追加しました。
ダイナミック ARP 検査機能	•「(2) ダイナミック ARP 検査オプション機能」の記述を変更しました。
DHCP snooping 使用時の注意事項	•「(3) 装置を再起動する場合について」を削除し，「(4) バインディングデータベースの保存と復元について」を追加しました。
バインディングデータベース保存の設定	• 本項を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 1.3（第 6 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
適合装置	下記のモデルを追加しました。 • AX-1230-24T2CA (AX1230S-24T2CA) • AX-1230-24P2CA (AX1230S-24P2CA)
本装置の特長	•「(9) OAN（Open Autonomic Networking）への対応」の記述を追加しました。
収容条件	•「(4) スパニングツリー」MST インスタンスごとの対象 VLAN 数を 200 に変更しました。 •「(8) 最大相手装置数（a）ARP エントリ数」を 1280 に変更しました。 •「(12) Web 認証」に最大認証数を追加しました。 •「(13) MAC 認証」に最大認証数を追加しました。
装置へのログイン	•「(3) 自動ログアウト」に set exec-timeout について記述を追加しました。
CLI の注意事項	•「(3) [Tab]，[?] による補完機能について」に固定文字列の補完について記述を追加しました。
オペレーション	• set exec-timeout コマンドを追加しました。
RADIUS を使用した認証	•「(3) RADIUS サーバの復旧」を追加しました。
システムファンクションリソース配分の設定	• Web 認証 /MAC 認証の固定 VLAN モードを追加しました。
1000BASE-X の解説	• 1000BASE-BX の記述を追加しました。
STP 互換モード	• 本項を追加しました。
スパニングツリー共通の注意事項	•「(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」を追加しました。
DHCP パケットの受信レート制限	• 本項を追加しました。
ダイナミック ARP 検査機能	• 本項を追加しました。
DHCP パケットの受信レートの設定	• 本項を追加しました。
ダイナミック ARP 検査機能の設定	• 本項を追加しました。
DHCP snooping の確認	• DHCP パケットの受信レート表示を追加しました。
ダイナミック ARP 検査の確認	• 本項を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 1.2（第 5 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
PoE の仕様	•「電力量」表記を，「電力の総和」「電力」に変更しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 1.2（第 4 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
収容条件	•「(5) DHCP snooping」を追加しました。 •「(12) Web 認証」に認証画面入れ替え時の条件を追加しました。
CLI の注意事項	• 注意事項「BackSpace キーについて」を削除しました。 • 注意事項「トレースモニタ使用時のコマンド入力について」を削除しました。
コンフィグレーション・運用コマンド一覧	• mkdir，rmdir コマンドを追加しました。
システムファンクションリソース配分の設定	• 本項を追加しました。
10BASE-T/100BASE-TX の解説	• ジャンボフレーム未サポートをサポートに訂正しました。(100BASE-TX 全二重だけ対象)
1000BASE-X 使用時の注意事項	• 1000BASE-SX2 サポートに伴う注意事項を追加しました。
PoE の仕様	• (3)PoE の給電停止についてを追加しました。
MAC ポートのオプション機能	• 本項を追加しました。
MAC ポートでの Tagged フレーム中継の設定	• 本項を追加しました。
DHCP snooping	• 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. 1.1（第 3 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
CLI の注意事項	• 注意事項を追加しました。
内蔵フラッシュメモリについて	• 本項を追加しました。
MAC アドレス学習の注意事項	• 本項を追加しました。
レイヤ 2 認証機能との連携について	• MAC 認証の端末 MAC アドレスについて追記しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 1.1（第 2 版）】

表　変更履歴

章・節・項・タイトル	追加・変更内容
適合装置	下記のモデルを追加しました。 • AX-1230-24P2C (AX1230S-24P2C) • AX-1230-48T2C (AX1230S-48T2C)
収容条件	•「(7) インタフェース数」の記述を変更しました。 •「(10) フィルタ・QoS」に layer2-2 モードと QoS の記述を追加しました。 •「(12) Web 認証」の記述を追加しました。 •「(13) MAC 認証」の記述を追加しました。
ログインセキュリティ	• RADIUS についての記述を追加しました。
イーサネット	• PoE についての記述を追加しました。
MLD snooping のコンフィグレーション	• MLD クエリーメッセージの送信元 IP アドレス設定の記述を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

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AX1200Sモデルを対象に記載しています。また，AX1200Sのソフトウェア Ver. 1.4の機能について記載しています。ソフトウェア機能は，ソフトウェアOS-LTによってサポートする機能について記載します。

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

■このマニュアルの訂正について

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

■対象読者

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

また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

■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。

http://www.alaxala.com

■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

AX1200S
ハードウェア取扱説明書
(AX12S-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の確認を知りたい

コンフィグレーションガイド
Vol.1
(AX12S-S001)
Vol.2
(AX12S-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
(AX12S-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
(AX12S-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
(AX12S-S005)

●MIBについて調べる

MIBレファレンス
(AX12S-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
(AX12S-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
CDP	Cisco Discovery Protocol
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System

CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
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
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MIB	Management Information Base
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point

NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PoE	Power over Ethernet
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

■常用漢字以外の漢字の使用について

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

を使用しています。

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

■ kB(バイト) などの単位表記について

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

目次

第 1 編　本装置の概要と収容条件

第 2 編　運用管理

第 4 編　レイヤ 2 スイッチ

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

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

本装置は，AX シリーズ製品ラインナップのローエンドとして，ファーストイーサネットによる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。

本装置は次の機能を実現します。

- ファーストイーサネットを収容し，PC を接続するファーストイーサネットによるシステム構築が可能
- 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 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
- 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

- ローエンドのファースト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，AX 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

（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※，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

注※

Ver.1.4 から認証モードの表記を変更しました。

- Ver.1.3.x まで：固定 VLAN モード，ダイナミック VLAN モード
- Ver.1.4 以降：固定 VLAN モード，ダイナミック VLAN モード，レガシーモード（レガシーモードは Ver.1.3.x までのダイナミック VLAN モードです。）

詳細は「コンフィグレーションガイド Vol.2」を参照してください。

● 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）などの標準機能と GSRP-aware 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

(6) 優れたネットワーク管理，保守・運用

- **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。
- **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**

(7) PoE 対応

- IEEE802.3af 準拠の PoE 対応
  IP 電話や無線アクセスポイントを直接収容できます。

(8) 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

(9) 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

AX1200S シリーズは 10/100BASE-TX ポートを最大 48 ポート，10/100/1000BASE-T ポートを最大 2 ポート装備し，高さを 1U に抑えたボックス型ファースト・イーサネットスイッチです。

標準のポート以外にアップリンクとして SFP スロット（最大 2 ポート）を装備し，1000BASE-SX，1000BASE-LX，1000BASE-LH，1000BASE-BX などを実装することができます。

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。

AX1200S シリーズは，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 認証機能などを備えています。

AX1200S シリーズには次に示すモデルがあります。

- AX1230S-24T2C，AX1230S-24T2CA
- AX1230S-24P2C，AX1230S-24P2CA
- AX1230S-48T2C

2.1.1 収容インタフェース数

本装置が収容できる最大インタフェース数を次の表に示します。

表 2-1 モデルごとのインタフェース数

インタフェース種別	モデル名		
	AX1230S-24T2C AX1230S-24T2CA	AX1230S-24P2C AX1230S-24P2CA	AX1230S-48T2C
1000BASE-X（SFP）	2※	2※	2※
10/100/1000BASE-T	2	2	2
10/100BASE-TX 【PoE 無】	24	－	48
10/100BASE-TX 【PoE 有】	－	24	－

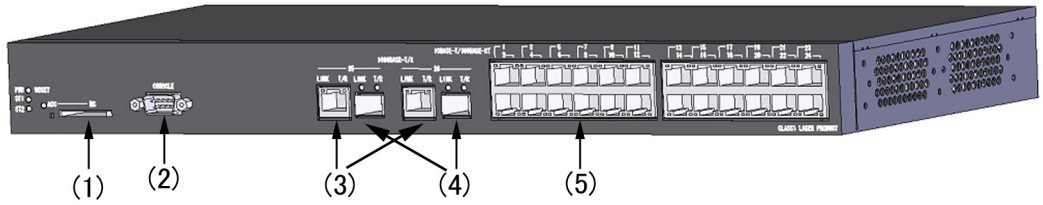
（凡例）－：未サポート

注※ 10/100/1000BASE-T のポートと排他使用になります（同時使用できません）。

2.1.2 装置の外観

装置外観図を次の図に示します。

図 2-1 AX1230S-24T2C，AX1230S-24T2CA，AX1230S-24P2C，AX1230S-24P2CA



(1) メモリカードスロット

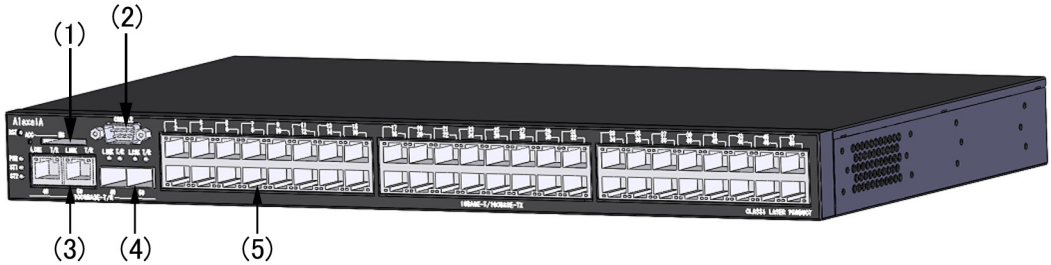
(2) CONSOLE ポート

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

(4) SFP モジュールスロット

(5) 10BASE-T/100BASE-TX イーサネットポート

図 2-2 AX1230S-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 モジュールスロット

(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　ハードウェアの構成

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。

図 2-3　ハードウェアの構成（AX1230S-24T2C，AX1230S-24T2CA モデル）

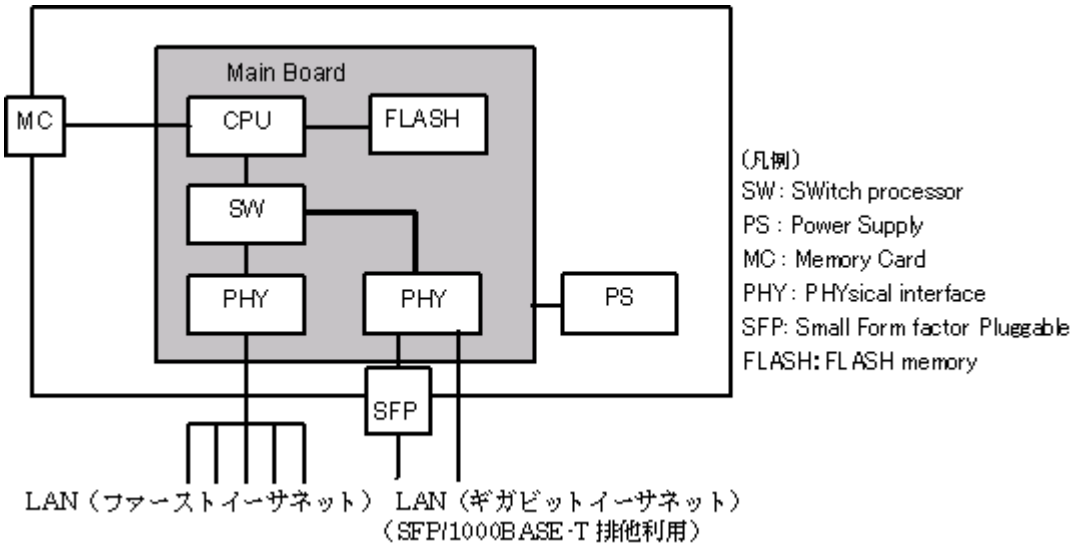


図 2-4　ハードウェアの構成（AX1230S-24P2C，AX1230S-24P2CA モデル）

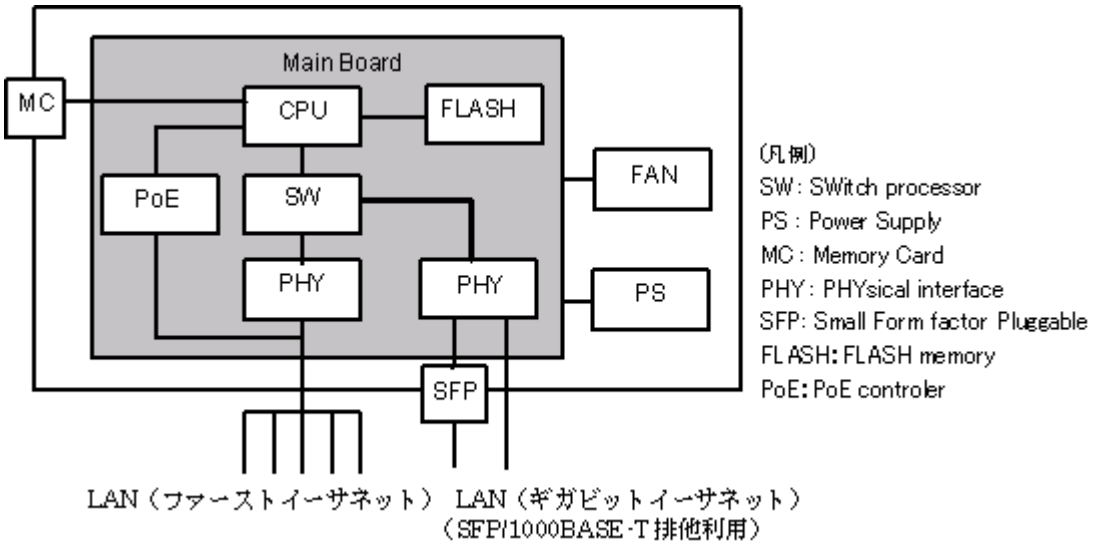
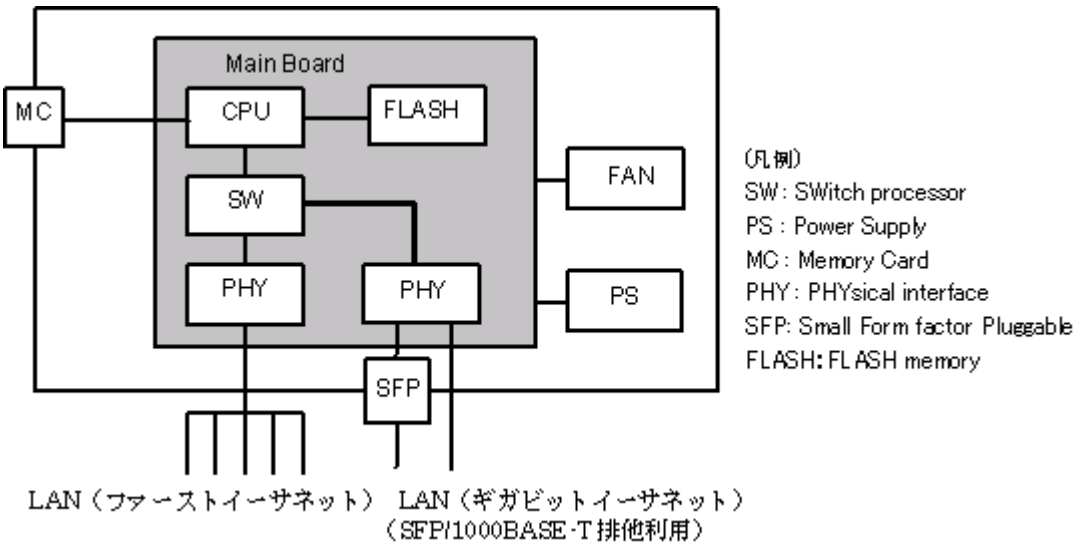


図 2-5 ハードウェアの構成（AX1230S-48T2C モデル）



（1） 装置筐体

装置筐体には，メインボード，PS，FAN が含まれています。

（2） メインボード

メインボードは CPU 部，SW 部，PHY 部から構成されます。

- CPU（Central Processing Unit）
  CPU を搭載し，装置全体の管理，SW 部 /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 CPU 部に搭載される装置内メモリに格納されます。
- 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。
- 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。
- PHY（Physical Interface）
  各種メディア対応のインタフェース部です。

（3） 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） FAN(AX1230S-24P2C，AX1230S-24P2CA，AX1230S-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。

（5） PoE(AX1230S-24P2C，AX1230S-24P2CA モデル)

LAN ケーブルを通じて受電側の機器へ電源を供給します。

2.2.2 ソフトウェア

本装置のソフトウェアを次の表に示します。

表 2-2 本装置のソフトウェア一覧

略称	内容
OS-LT	AX1200S 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

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

3.1.1 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			
	1000BASE-X(SFP)	10/100/1000BASE-T	10/100BASE-TX【PoE 無】	10/100BASE-TX【PoE 有】
AX1230S-24T2C AX1230S-24T2CA	2	2※	24	－
AX1230S-24P2C AX1230S-24P2CA	2	2※	－	24
AX1230S-48T2C	2	2※	48	－

（凡例）－：該当なし。

注※

1000BASE-X（SFP) と排他使用 (同時使用不可）です。

1000BASE-X（SFP) を使用しない場合の最大回線数であり，1000BASE-X（SFP) を使用した場合は，その使用回線数分マイナスした値になります。

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	AX1200S シリーズ
メインボード搭載メモリ量(RAMDISK 含む)	64MB （内，RAMDISK は 6MB)
内蔵フラッシュメモリ容量	8MB
MC 容量	128MB

(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。

たと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

(1) 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 3-3 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

(2) 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 3-4 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	8192※	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 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。

(3) 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 3-5 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
AX1230S-24T2C AX1230S-24T2CA	256	256	6656
AX1230S-24P2C AX1230S-24P2CA			6656
AX1230S-48T2C			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 3-6 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 3-7 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 3-8 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。

(4) 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 3-9 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 3-10 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 3-11 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。

（5） DHCP snooping

DHCP snooping の収容条件を次の表に示します。

表 3-12 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。

（6） 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 3-13 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。

（7） インタフェース数

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

（a） 最大インタフェース数

本装置でサポートする最大インタフェース数を次の表に示します。

表 3-14 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

（b） 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。

（c） IP アドレス最大設定数

(i) IPv4 アドレス

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

表 3-15 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

（8） 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 3-16 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	1280	1280

(9) 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 3-17 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。

(10) 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共通モードである受信側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。

(a) 受信側フィルタエントリ数

受信側フロー検出モードlayer2-1またはlayer2-2のいずれかを選択した場合に設定できるフィルタ最大エントリ数を次の表に示します。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 3-18 モードlayer2-1，layer2-2の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

(b) 受信側 QoS エントリ数

受信側フロー検出モード 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 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 3-19 モード layer2-1，layer2-2 の 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

(11) レイヤ 2 認証機能

装置全体の認証端末数を次の表に示します。

表 3-20 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 3-21 その他のレイヤ２認証共通機能収容条件

項目	最大数
RADIUS サーバ登録数	4※
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	20

注※
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。

（a） IEEE802.1X

IEEE802.1X の収容条件を次の表に示します。

表 3-22 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	認証失敗端末最大登録可能数※3
ポート単位認証	(静的)	64	不可			256	不可	256
	(動的)	64	不可			256	不可	256
VLAN 単位認証	(動的)			256	不可	256	不可	256
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	256

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。

注※ 3
認証失敗端末が 256 となったとき，新規認証要求端末の処理は実施できません。この場合，新規認証要求端末の処理が実施可能となるのは，認証失敗端末の管理エントリがタイムアウトにより消失したときとなります。

表 3-23 IEEE802.1X の収容条件

項目		最大数
最大 IEEE802.1X 設定可能物理ポート数	AX1230S-24T2C，AX1230S-24T2CA	26
	AX1230S-24P2C，AX1230S-24P2CA	26
	AX1230S-48T2C	50
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※1
	MAC VLAN へ MAC アドレススタティック登録	64/ 装置※2

注※ 1
MAC アドレステーブルのスタティックエントリ数です。

注※ 2
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。

（b） Web 認証

Web 認証の収容条件を次の表に示します。

表 3-24　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	認証失敗端末最大登録可能数※3
固定 VLAN モード	1024	可			1024	可	ー
ダイナミック VLAN モード	256	可			256	可	ー
レガシーモード			256	不可	256	可	ー
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	ー

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。

注※ 3

Web 認証では認証失敗端末を管理していないため，失敗端末登録可能数は存在しません。

表 3-25　Web 認証の収容条件

項目		最大数
内蔵 Web 認証 DB 登録ユーザ数		300※1
同時認証数		10
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※2
認証画面入れ替えで指定できるファイル数		64※3
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

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※ 2

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※ 3

ファイル名にピリオド（.）や拡張子（txt など）を含んで 13 文字を超えるファイルが存在する場合，ファイル数の上限はさらに少なくなります。

(c) MAC 認証

MAC 認証の収容条件を次の表に示します。

表 3-26 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	認証失敗端末最大登録可能数※3
固定 VLAN モード	1024	可			1024	可	1024
ダイナミック VLAN モード	256	可			256	可	256
レガシーモード			256	不可	256	可	256
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	1280

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。

注※ 3

MAC 認証の認証失敗端末が，固定 VLAN モード 1024，またはダイナミック VLAN モード 256 となったとき，それぞれのモードの新規認証要求端末の処理は実施できません。この場合，新規認証要求端末の処理が実施可能となるのは，認証失敗端末の管理エントリがタイムアウトにより消失したときとなります。

表 3-27 MAC 認証の収容条件

項目	最大数
内蔵 MAC 認証 DB 登録 MAC アドレス数	1024
同時認証数	20

(12) IEEE802.3ah/UDLD

IEEE802.3ah/UDLD の収容条件を次の表に示します。

表 3-28 IEEE802.3ah/UDLD の収容条件

モデル	最大リンク監視情報数
AX1230S-24T2C AX1230S-24T2CA	26
AX1230S-24P2C AX1230S-24P2CA	26
AX1230S-48T2C	50

（13）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 3-29　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

（14）隣接装置情報（LLDP）の収容条件

隣接装置情報（LLDP）の収容条件を次の表に示します。

表 3-30　隣接装置情報（LLDP）の収容条件

項目	最大収容数
LLDP 隣接装置情報	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

4.1.1 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

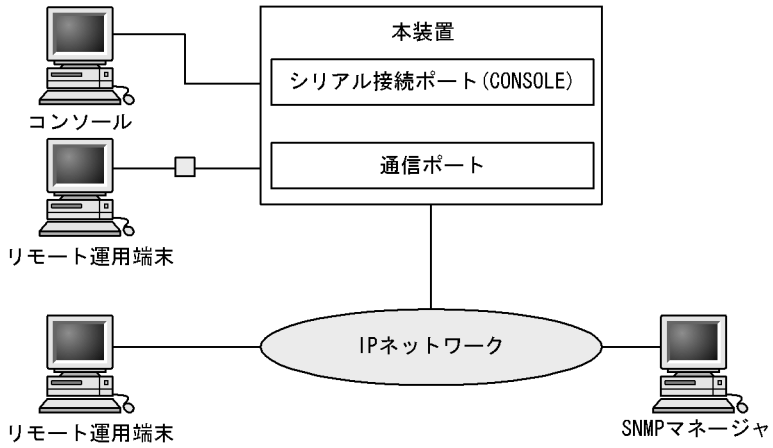


表 4-1　運用端末の条件

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。

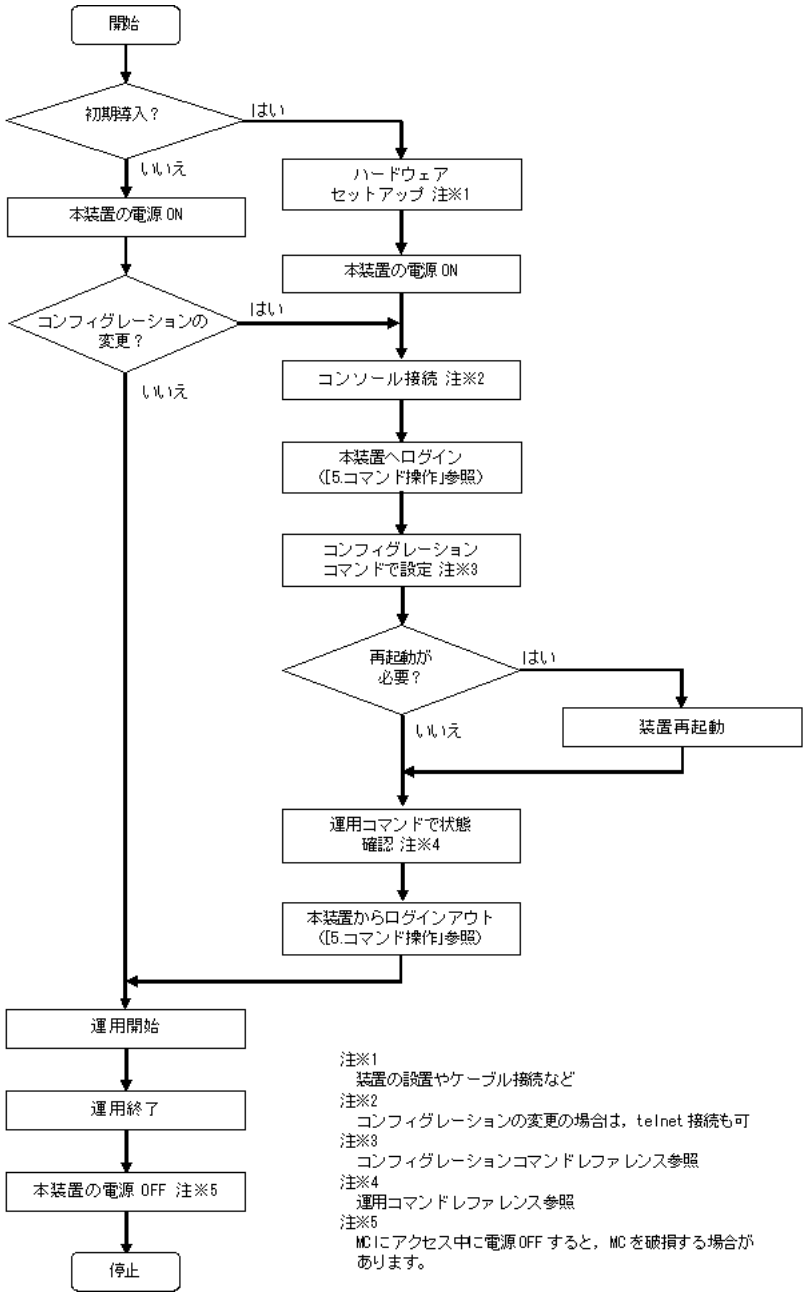
4.2　装置起動

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。	本体の電源スイッチを ON にします。
リセットによる再起動	障害発生などにより，本装置をリセットしたい場合に行います。	本体のリセットスイッチを押します。
コマンドによる再起動	障害発生などにより，本装置をリセットしたい場合に行います。	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。

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) 2006,2008, 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，[Enter] だけを押下してください。
   また，パスワードの入力文字は表示しません。
2. コマンドプロンプトを表示します。

(2) ログアウト

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

図 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

5.1.1 運用コマンド一覧

コマンド入力モードの切り換えおよびユーティリティに関する運用コマンド一覧を次の表に示します。

表 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。

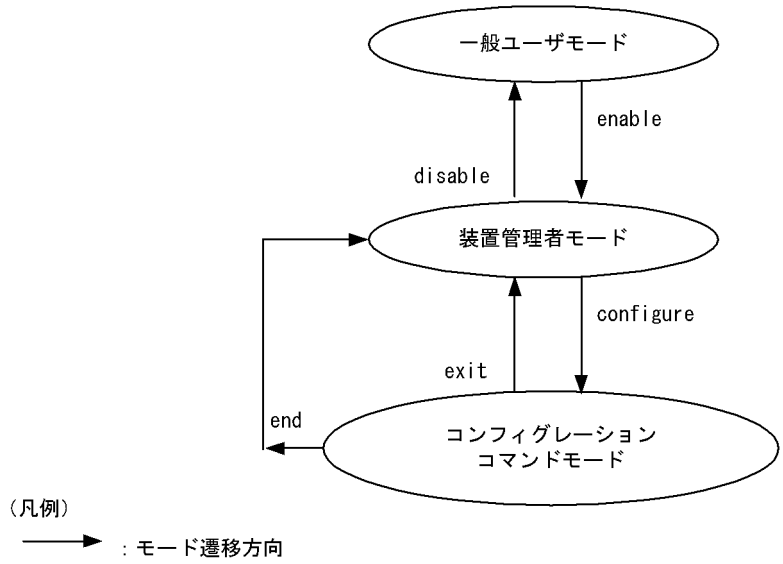
コマンド入力モードとプロンプトの対応を次の表に示します。

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 でホスト名称を設定している場合，プロンプトに反映されます。
2. ランニングコンフィグレーションを編集し，その内容をスタートアップコンフィグレーションファイルに保存していない場合，プロンプトの先頭に「！」が付きます。

1. ～ 2. 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

```
OFFICE1# configure
OFFICE1(config)# system function filter qos dhcp-snooping
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ファイル名の入力を少なくすることができ，コマンド入力が簡単になります。補完機能を使用したコマンド入力の簡略化を次の図に示します。

図 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　30　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 2006/12/13 22:29:54 UTC
Total: 2
IP Address      Linklayer Address  Interface  Expire     Type
192.168.10.99   0013.20a5.3e2e     VLAN0001   18min      arpa
200.1.100.1     0071.0100.0001     VLAN3001   19min      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。（デフォルト：30 コマンドまで）
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。
Ctrl ＋ K	カーソルの後ろのテキストを削除します。

キーボード	本装置の動作
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。

(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＞ 固定キーワード

＜可変値＞を入力後，入力不可能な固定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) 補完しないパラメータ（固定文字列キーワード）

任意の文字列または固定文字列キーワードを選択して入力する場合，固定文字列キーワードの一部を入力しても [Tab] で補完しないコマンドがあります。

図 5-12 補完しないパラメータ例（固定文字列キーワード）

```
# remove web-authentication user [？]
 <WA user name | -all>   - {<Web auth user name> | -all}: [1-16] characters or "
                           -all"
# remove web-authentication user -[Tab]
# remove web-authentication user -          ••• 補完しないで入力行を再表示
```

本例は任意の文字列 <Web auth user name> と固定文字列キーワード "-all" の択一ですが，"-" や "-a" に続いて [Tab] を入力しても "-all" に補完しません。

(d) 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) コンフィグモードでの入力について

コンフィグモード（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

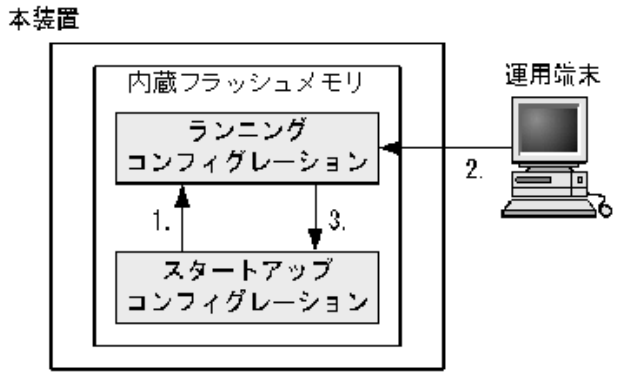
運用開始時または運用中，ネットワークの運用環境に合わせて，本装置に接続するネットワークの構成および動作条件などのコンフィグレーションを設定する必要があります。初期導入時，コンフィグレーションは設定されていません。

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。

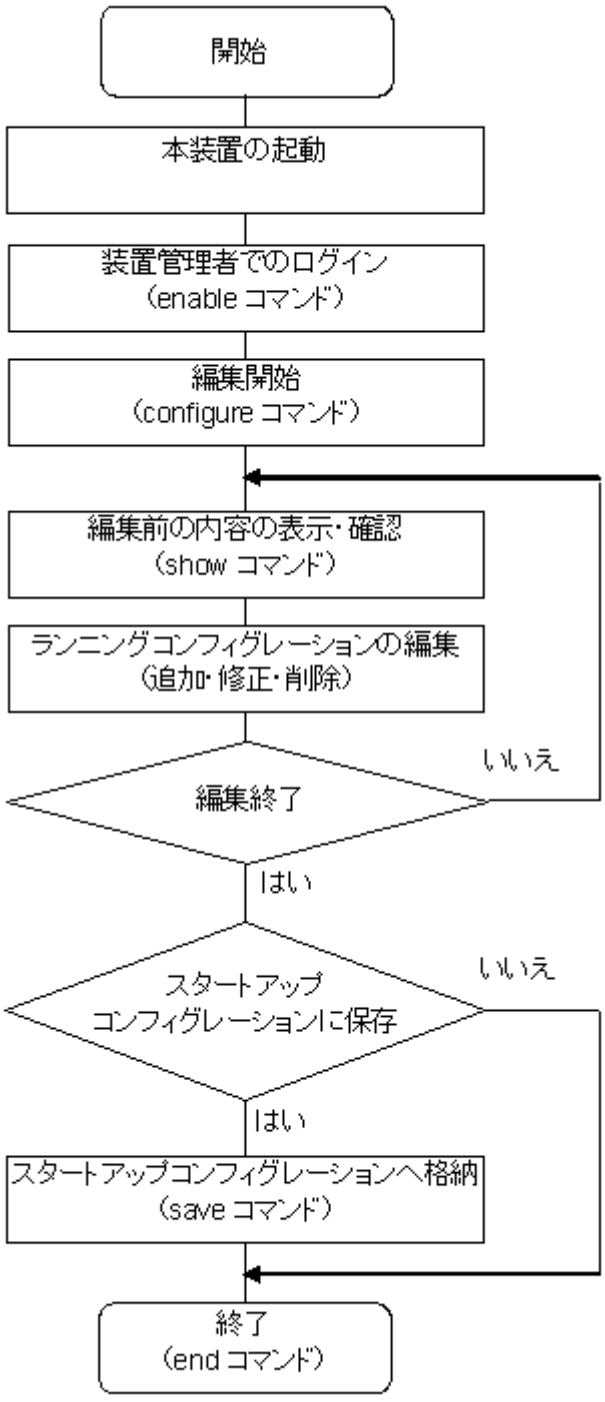
6.1.2 運用中のコンフィグレーション

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。

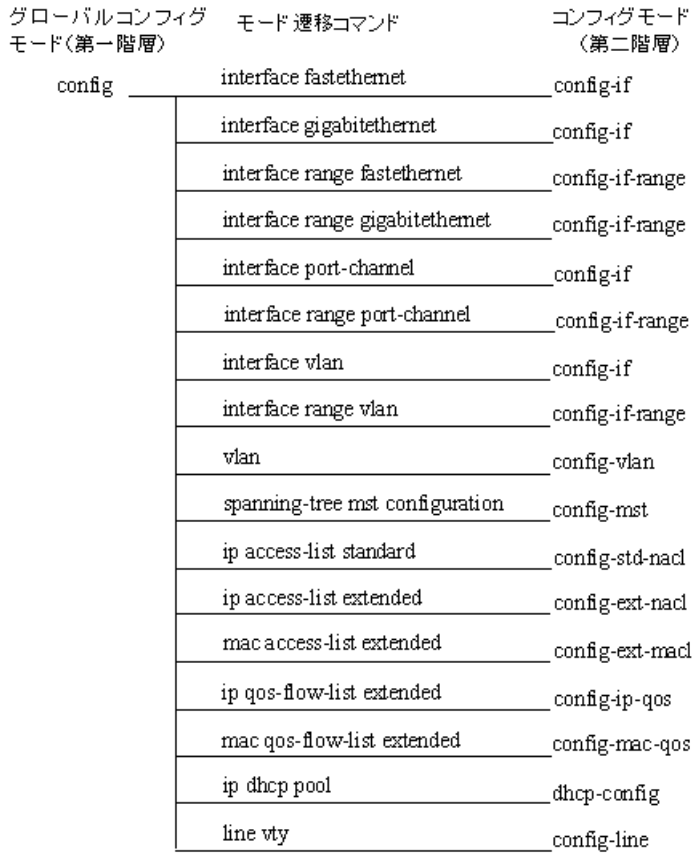
図 6-2　ランニングコンフィグレーションの編集の流れ



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 AX1230S-24T2C
!
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 AX1230S-24T2C
!
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。（WindowsXP 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 ax12sconf.txt 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 ax12sconf.txt
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 ax12sconf.txt
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。

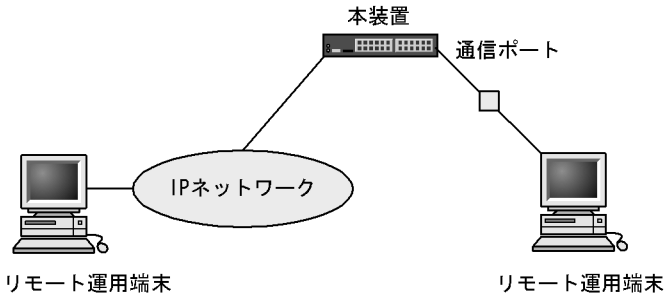
7 リモート運用端末から本装置へのログイン

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

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。

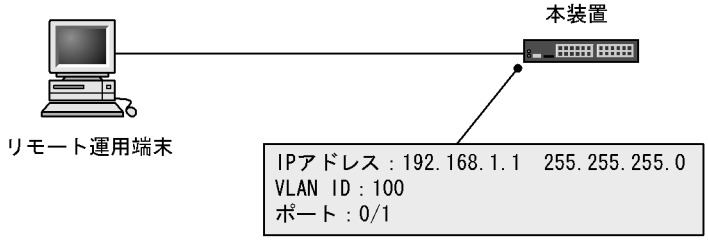
VLAN の設定，および IPv4 インタフェースの設定に関するコンフィグレーションコマンドについては，「15 VLAN」，「21 IPv4 インタフェース」を参照してください。

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。
line console speed	コンソール（RS-232C）の通信速度を変更します。
trace-monitor	イベントトレースのモニタ表示実施／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，「21 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

8.1.1 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。
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。

8.1.3 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)#
```

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)#
```

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)# permit src 192.168.0.0 0.0.0.255
   (config-std-nacl)# deny src 192.168.0.254 0.0.0.0
   (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

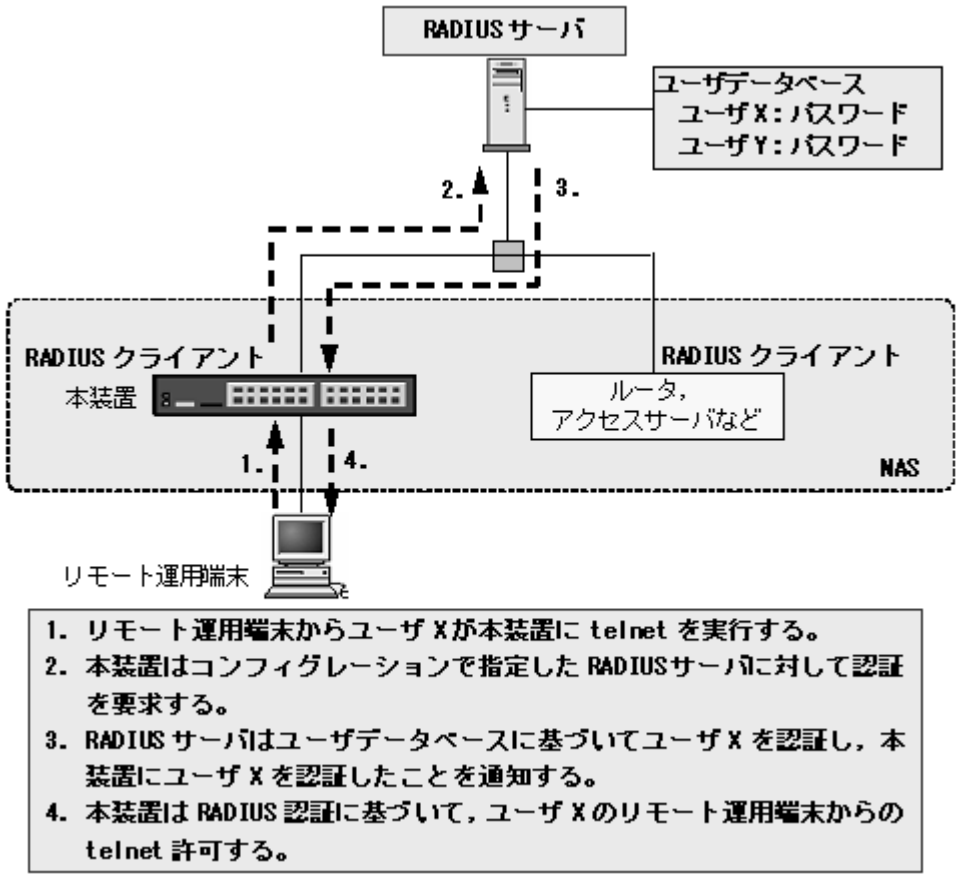
8.2.1　RADIUS の概要

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）
- レイヤ 2 認証機能（IEEE802.1X，Web 認証，MAC 認証）

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)
属性	ログイン認証で使用する次の属性 • User-Name • User-Password • Service-Type • NAS-IP-Address • NAS-Identifier

（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。

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。
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。
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。

- 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 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。

8.2.3 RADIUS を使用した認証

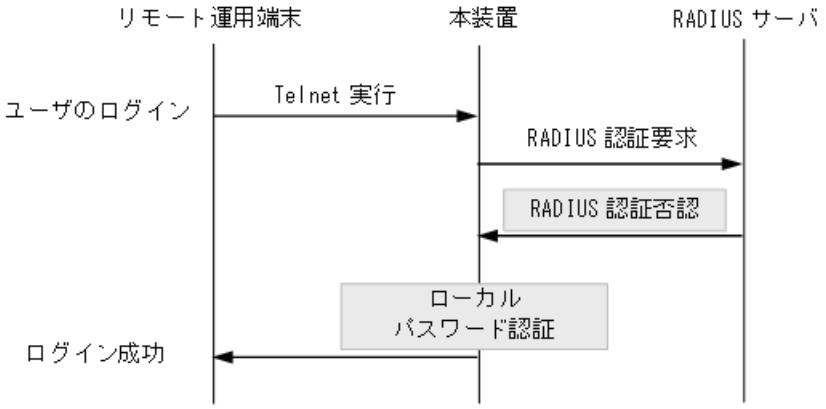
RADIUS を使用した認証方法について説明します。

(1) ログイン認証サービスの選択

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。これらの認証方式は単独でも同時でも指定でき，同時に指定された場合は先に指定された方式で認証に失敗した場合に，次に指定された方式で認証できます。

認証方式として RADIUS 認証，ローカルパスワード認証の順番で指定した場合の認証方式シーケンスを次の図に示します。

図 8-7 認証方式シーケンス



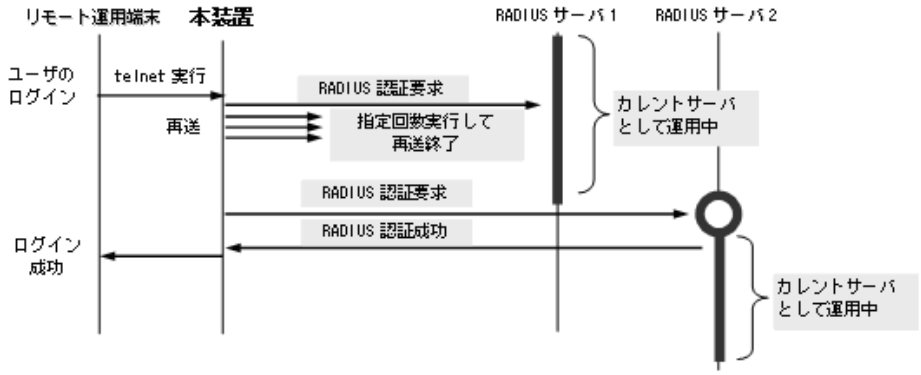
この図では端末からユーザが本装置に telnet を実行すると，RADIUS サーバに対し本装置から RADIUS 認証を要求します。RADIUS サーバと通信不可または RADIUS サーバでの認証に失敗すると，次に本装置のローカルパスワード認証機能での認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

(2) RADIUS サーバの選択

RADIUS サーバは最大 4 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。RADIUS サーバ選択のシーケンスを次の図に示します。

図 8-8　RADIUS サーバ選択のシーケンス



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

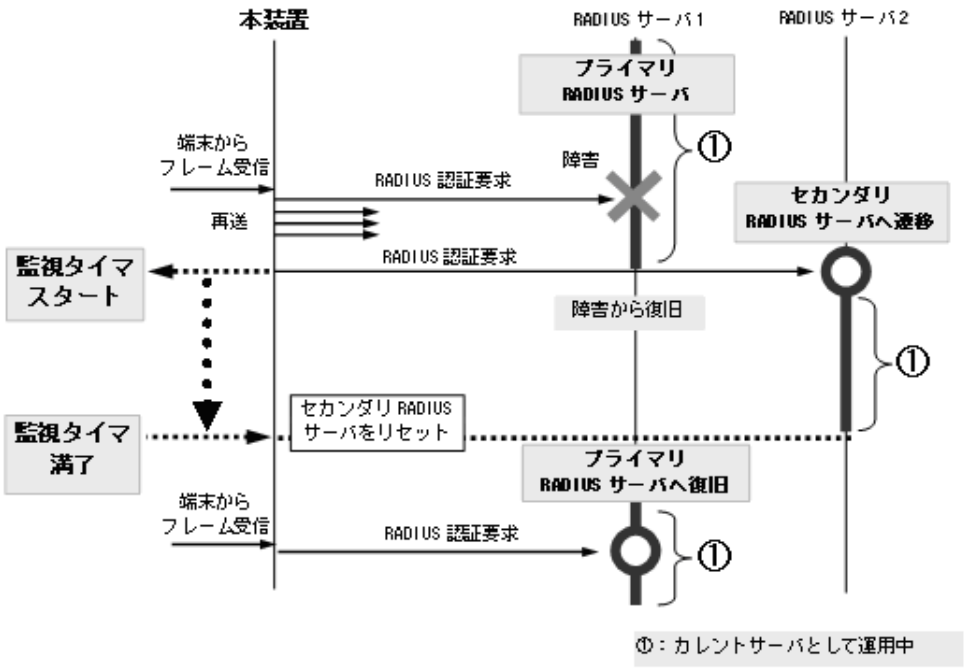
また，認証要求先として運用中の RADIUS サーバをカレントサーバと呼びます。

（3） RADIUS サーバの復旧

本装置は 1 台目の端末からのパケット受信による 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。

最初の RADIUS サーバ（プライマリ RADIUS サーバ）の自動復旧手段として，監視タイマによる自動復旧機能をサポートします。プライマリ RADIUS サーバへの復旧シーケンスを次の図に示します。

図 8-9　プライマリ RADIUS サーバへの復旧シーケンス (1)



1. 認証要求先として運用中の RADIUS サーバをカレントサーバと呼びます。
2. 運用コマンド show radius-server summary で最初に表示する RADIUS サーバを，プライマリ RADIUS サーバ※1 と呼びます。
   プライマリ RADIUS サーバをカレントサーバとして RADIUS 認証要求を開始します。
3. プライマリ RADIUS サーバに障害が発生して，次に有効な RADIUS サーバへ遷移した場合，その RADIUS サーバをセカンダリ RADIUS サーバと呼びます。
4. カレントサーバがセカンダリ RADIUS サーバに遷移した時点で監視タイマをスタートします。
5. 最後の有効な RADIUS サーバへ認証要求ができなかったときは認証失敗※2 とし，この状態をカレントサーバ※3 として監視タイマをスタート※4 します。（監視タイマをスタート済みのときは継続します。）
6. 監視タイマが満了すると，カレントサーバはプライマリ RADIUS サーバへ復旧します。
7. 監視タイマ満了後にプライマリ RADIUS サーバへ復旧してもプライマリ RADIUS サーバが障害から復旧していない場合，再度有効な RADIUS サーバ選択処理を実行します。カレントサーバが有効なセカンダリ RADIUS サーバへ遷移した時点で，再度監視タイマをスタートします。

注※1

コンフィグレーションコマンド radius-server host で設定した RADIUS サーバは，以下のいずれかの条件を満たしている設定が有効です。

- radius-server host の key パラメータの設定有
- radius-server host の key パラメータの設定無だが，radius-server key 設定有

上記の条件を満たしていない RADIUS サーバ設定は無効となり，最初に設定されていてもプライマリ RADIUS サーバとなりません。

注※2

レイヤ 2 認証機能の場合は，強制認証または認証失敗となります。レイヤ 2 認証機能の強制認証については，「コンフィグレーションガイド Vol.2」の各認証機能の解説編を参照してください。

注※3

運用コマンド show radius-server summary では，「* RADIUS server unreachable」を表示します。

注※4

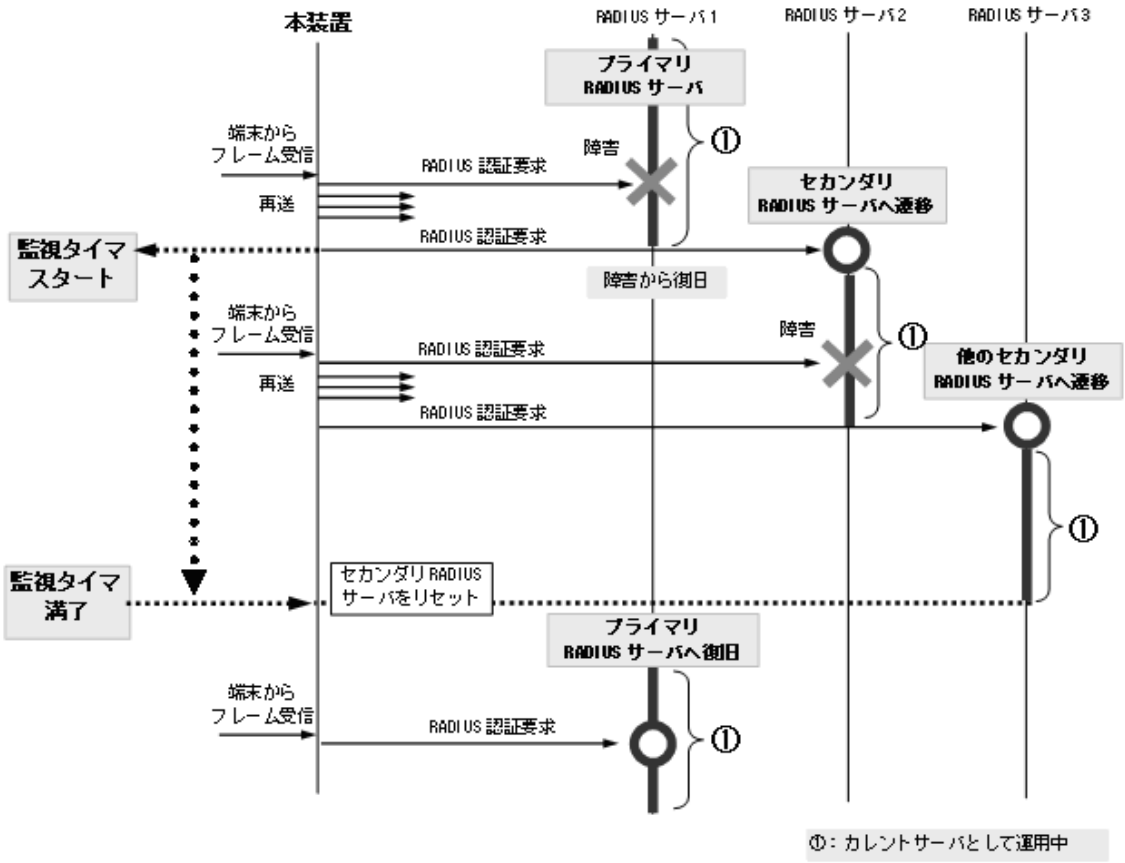
このときの監視タイマが満了するまでは，RADIUS サーバへ認証要求を送信しないで，認証失敗（レイヤ 2 認証機能は強制認証または認証失敗）として扱います。（コンフィグレーションコマンド radius-server dead-interval 0 設定のときは，監視タイマをスタートしないで，プライマリ RADIUS サーバへ復旧します。）

また，監視タイマはいったんスタートすると基本的には満了するまでリセットしません。

下記のように 3 台以上の RADIUS サーバを設定した環境で監視タイマをスタート後に，別の RADIUS サーバにカレントサーバが遷移した場合でも，監視タイマはリセットせずに満了するまで継続します。

3 台以上の RADIUS サーバを設定した場合のシーケンスを次の図に示します。

図 8-10　プライマリ RADIUS サーバへの復旧シーケンス (2)



なお，下記の契機では例外として満了せずにリセットします。

- コンフィグレーションコマンドで radius-server dead-interval 0 を設定したとき
- カレントサーバとして運用中の RADIUS サーバ情報を，コンフィグレーションコマンド radius-server host で削除したとき
- 運用コマンド clear radius-server を実行したとき

（4） ログインユーザ情報

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。

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
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 RADIUS サーバを設定します。
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。

8.3.2 RADIUS サーバによる認証の設定

［設定のポイント］

本例では，RADIUS 認証，およびローカルパスワード認証を行う設定例を示します。RADIUS 認証に失敗した場合には，本装置によるローカルパスワード認証を行うように設定します。
あらかじめ，通常のリモートアクセスに必要な設定を行っておく必要があります。

［コマンドによる設定］

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

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

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 summary	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 サーバの確認

(1) 有効 RADIUS サーバの表示

運用コマンド show radius-server summary 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「* RADIUS server unreachable」を表示します。

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

```
> show radius-server summary

Date 2008/11/11 02:42:12 UTC
   IP address:192.168.0.203 [Tx] Timeout:45 [Rx] Accept:0, Reject:0
   IP address:192.168.0.202 [Tx] Timeout:50 [Rx] Accept:0, Reject:0
   IP address:192.168.0.201 [Tx] Timeout:96 [Rx] Accept:0, Reject:0
 * IP address:192.168.0.200 [Tx] Timeout:0 [Rx] Accept:1024, Reject:0
 * : Current server

>
```

図 8-12 show radius-server summary の実行結果（全 RADIUS サーバ使用不可）

```
> show radius-server summary

Date 2008/11/11 02:34:20 UTC
   IP address:192.168.0.203 [Tx] Timeout:1 [Rx] Accept:0, Reject:0
   IP address:192.168.0.202 [Tx] Timeout:1 [Rx] Accept:0, Reject:0
   IP address:192.168.0.201 [Tx] Timeout:1 [Rx] Accept:0, Reject:0
   IP address:192.168.0.200 [Tx] Timeout:1 [Rx] Accept:0, Reject:0
 * RADIUS server unreachable
 * : Current server

>
```

「*」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

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

図 8-13　show radius-server statistics の実行結果（有効 RADIUS サーバで動作中）

```
> show radius-server statistics

Date 2008/11/11 02:42:14 UTC
   IP address: 192.168.0.203    Port: 1812  Current Request: 0
    [Tx] Request  :         45  Error  :        101
         Retry    :          0  Timeout:         45
    [Rx] Accept   :          0  Reject :          0  Challenge  :          0
         Malformed:          0  BadAuth:          0  UnknownType:          0
   IP address: 192.168.0.202    Port: 1812  Current Request: 0
    [Tx] Request  :         50  Error  :         96
         Retry    :          0  Timeout:         50
    [Rx] Accept   :          0  Reject :          0  Challenge  :          0
         Malformed:          0  BadAuth:          0  UnknownType:          0
   IP address: 192.168.0.201    Port: 1812  Current Request: 0
    [Tx] Request  :         96  Error  :         50
         Retry    :          0  Timeout:         96
    [Rx] Accept   :          0  Reject :          0  Challenge  :          0
         Malformed:          0  BadAuth:          0  UnknownType:          0
 * IP address: 192.168.0.200    Port: 1812  Current Request: 0
    [Tx] Request  :       1024  Error  :          0
         Retry    :          0  Timeout:          0
    [Rx] Accept   :       1024  Reject :          0  Challenge  :          0
         Malformed:          0  BadAuth:          0  UnknownType:          0
 * : Current server

>
```

図 8-14　show radius-server statistics の実行結果（全 RADIUS サーバ使用不可）

```
> show radius-server statistics

Date 2008/11/11 02:47:29 UTC
   IP address: 192.168.0.203    Port: 1812  Current Request: 0
    [Tx] Request  :         93  Error  :        147
         Retry    :          0  Timeout:         93
    [Rx] Accept   :          0  Reject :          0  Challenge  :          0
         Malformed:          0  BadAuth:          0  UnknownType:          0
   IP address: 192.168.0.202    Port: 1812  Current Request: 0
    [Tx] Request  :        101  Error  :        139
         Retry    :          0  Timeout:        101
    [Rx] Accept   :          0  Reject :          0  Challenge  :          0
         Malformed:          0  BadAuth:          0  UnknownType:          0
   IP address: 192.168.0.201    Port: 1812  Current Request: 0
    [Tx] Request  :        133  Error  :        107
         Retry    :          0  Timeout:        133
    [Rx] Accept   :          0  Reject :          0  Challenge  :          0
         Malformed:          0  BadAuth:          0  UnknownType:          0
   IP address: 192.168.0.200    Port: 1812  Current Request: 0
    [Tx] Request  :        240  Error  :          0
         Retry    :          0  Timeout:        240
    [Rx] Accept   :          0  Reject :          0  Challenge  :          0
         Malformed:          0  BadAuth:          0  UnknownType:          0
 * RADIUS server unreachable
 * : Current server

>
```

「*」は現在使用中の RADIUS サーバの IP アドレスを示します。

9 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。

9.1 装置の状態確認，および運用形態に関する設定

9.1.1 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 9-1 コンフィグレーションコマンド一覧

コマンド名	説明
system function	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。

表 9-2 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，電源状態，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 9-3 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 9-4 運用コマンド一覧（ログ情報の確認）

コマンド名	説明
show event-trace	イベントトレースを採取時間・メッセージだけを一覧表示します。
clear event-trace	本装置で収集しているイベントトレースを消去します。
show log	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 log	本装置で収集しているログを消去します。

9.1.2 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 9-1 ソフトウェア情報の確認

```
> show version

Date 2008/07/20 12:03:40 UTC

Model and S/W version
  AX1230S-24T2C Ver.1.4 (Build:xx)

H/W Serial Number:
  xxxxxxxxxxxxxxxx

H/W Revision: x

>
```

9.1.3 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 9-2 装置の状態確認

```
> show system

Date 2008/07/30 01:03:02 UTC
System: AX1230S-24T2C Ver. 1.4 (Build:yy)
    Name         : -
    Contact      : -
    Locate       : -
    Machine ID   : 00ee.f025.0001
    Boot Date    : 2008/07/24 09:31:07
    Elapsed time : 5 days 15:31:55
    LED
       ST1 LED   : Green

Environment
    Fan          : -
    Temperature  : normal
    Accumulated running time
       total     : 489 days and 12 hours
       critical  : 5 days and 17 hours

File System
    < RAMDISK information >
       used        41,984 byte
       free     6,249,472 byte
       total    6,291,456 byte
    < RAMDISK files >
     There is no file. ( RAMDISK )
    < MC information >
    MC : enable
    Manufacture ID : 00000003
       used    10,534,400 byte
       free   115,376,128 byte
       total  125,910,528 byte
    < MC files >
    File Date               Size Name
    2008/07/24 13:07   5,232,640 K.IMG
    2008/07/24 13:07   5,232,640 AX12L20104-xx.bin

System Setting
    set terminal pager : enabled   (save: enabled)
    line console speed : 9600      (save: 9600)
```

```
    trace-monitor       : disabled  (save: enabled)
    set exec-timeout    : 0         (save: 0)

Device Resources
    IP Routing Entry(static)     :    0(max entry=128)
    IP Routing Entry(connected)  :    2(max entry=128)
    IP Interface Entry           :    2(max entry=128)
    IP ARP Entry                 :    0(max entry=1280)
    MAC-address Table Entry      :   32(max entry=8192)

    System Function Resources : 1/7(Used/Max)
    System Layer2 Table Mode  : auto (mode=1)
    Flow detection mode : layer2-2
      Used resources for filter(Used/Max)
                              MAC      IPv4
        Port 0/1-26     :       -     0/128
        VLAN            :       -     0/128
      Used resources for QoS(Used/Max)
                              MAC      IPv4
        Port 0/1-26     :       -      0/64
        VLAN            :       -      0/64

>
```

9.1.4 イベントトレース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イベントトレースメッセージとして運用端末（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メッセージを，通信停止状態になった場合は通信停止状態になったメッセージを表示します。

図 9-3 イベントトレース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 9-4 イベントトレースのモニタ表示の停止

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

注意

多数のイベントトレースが連続して発生した際，コンソール上には一部しか表示しませんので，運用コマンド show event-trace で確認してください。

9.1.5 イベントトレース・装置障害ログ情報の確認

イベントトレースは運用端末（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。

イベントトレース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情報で，運用端末のモニタ表示と同様の内容が格納されます。イベントトレース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

これらの情報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 event-trace 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 log で確認できます。

9.1.6 システムファンクションリソース配分の設定

本装置でサポートしている機能のうち，下記の機能についてはシステムファンクションリソース（以下，システムリソースと称す）を使用します。装置として同時に使用できるリソース数は最大 7 個です。システムリソースの使用数は各機能により異なります。

表 9-5 システムリソースを必要とする機能とリソース数

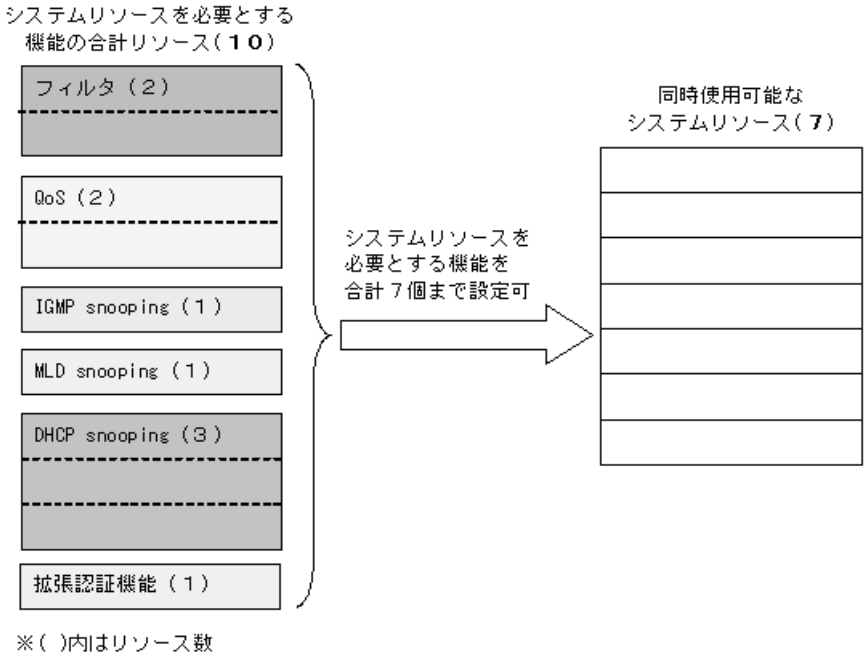
機能	機能概要		必要リソース数	備考
フィルタ	MAC 拡張アクセスリスト IP 標準アクセスリスト IP 拡張アクセスリスト		2	デフォルトで使用可
QoS	MAC QoS フロー検出 IP QoS フロー検出		2	デフォルトで使用可
IGMP snooping	IPv4 マルチキャスト制御		1	デフォルトで使用可
MLD snooping	IPv6 マルチキャスト制御		1	デフォルトで使用可
DHCP snooping	DHCP パケット制御 端末フィルタ		3	デフォルトで使用不可
拡張認証機能 （レイヤ 2 認証）	認証機能共通	• 認証専用 IPv4 アクセスリスト	1	デフォルトで使用不可
	IEEE802.1X	• ポート単位認証（動的）		
	Web 認証	• 固定 VLAN モード • ダイナミック VLAN モード • Web 認証専用 IP アドレス		
	MAC 認証	• 固定 VLAN モード • ダイナミック VLAN モード		

装置の最大リソース数の制限上，上記に示す機能すべてを同時に使用することはできません。ネットワーク構成に合わせて設定段階の最初にリソース配分パターンを設定する必要があります。配分パターンはコンフィグレーションコマンド system function で指定できます。

［注意事項］

1. DHCP snooping，拡張認証機能を使用する場合は，コンフィグレーションコマンド system function 設定が必要です。（その他の機能は，コマンド未設定でも使用可能です。）
2. 本設定は装置としてシステムリソースを使用する基本条件を設定するものです。必ず運用開始前の最初の段階で設定してください。（設定後は装置の再起動が必要です。）
3. 各機能に関連する設定がある場合，リソース配分の変更はできません。先に各機能関連の設定をすべて削除してから，配分の変更を行ってください。
4. 最大リソース数を超える割り当てを指定した場合は，コンフィグレーションコマンドでエラーとなり設定できません。

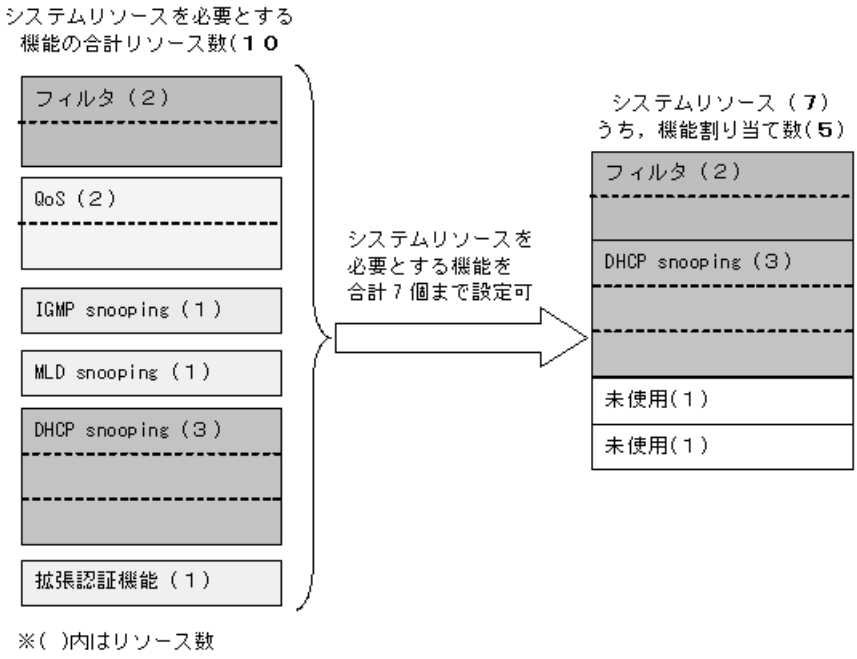
図 9-5 システムリソース割り当て概要



(1) システムリソース最大数以内での割り当て

システムリソース数は必ず最大７個まで割り当てる必要はありません。最大数以内であれば，未使用リソースがあっても問題ありません。

図 9-6 システムリソース割り当て例１



［設定のポイント］

フィルタ機能と DHCP snooping 機能を使用する場合は，コンフィグレーションコマンド system function で filter と dhcp-snooping を設定します。（合計５個使用）

［コマンドによる設定］

1. **(config)# system function filter dhcp-snooping**
   Please execute the reload command after save,
   because this command becomes effective after reboot.
   フィルタ機能と DHCP snooping 機能を設定します。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。

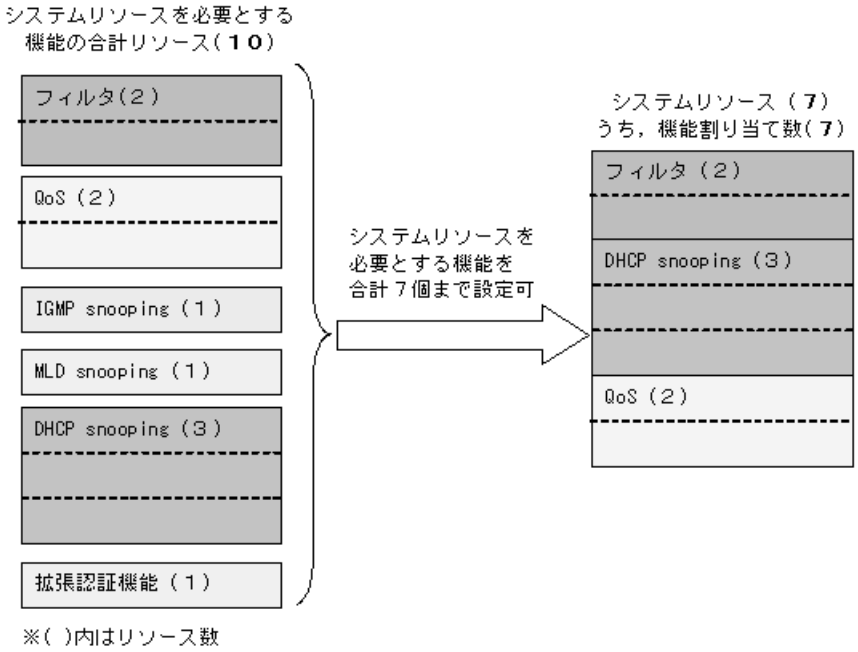
3. **@# reload**
   Restart OK? (y/n): **y**
   コンフィグレーションの設定を保存すると，プロンプトに " @ " を表示しますので，運用コマンド reload で装置を再起動してください。

［注意事項］
この場合，QoS および IGMP/MLD snooping，拡張認証機能は使用できません。

（2） システムリソース最大数の割り当て

システムリソース数を最大 7 個まで割り当てることが可能です。

図 9-7 システムリソース割り当て例 2（最大数割り当て）



［設定のポイント］
フィルタ機能，QoS 機能と DHCP snooping 機能を使用する場合は，コンフィグレーションコマンド system function で filter，qos と dhcp-snooping を設定します。（合計 7 個使用）

［コマンドによる設定］

1. **(config)# system function filter qos dhcp-snooping**

```
Please execute the reload command after save,
because this command becomes effective after reboot.
```

フィルタ機能，QoS 機能と DHCP snooping 機能を設定します。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］

この場合，IGMP/MLD snooping，拡張認証機能は使用できません。

9.2　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。

対象情報は，次に示す「9.2.2　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。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。

9.2.1　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 9-6　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 に保存します。
restore	MC に保存している装置情報を本装置に復元します。

9.2.2　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 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 9-7　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	
ログインユーザ ID ／ログインパスワード	
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
イベントトレースのモニタ表示設定	運用コマンド trace-monitor
装置の障害ログ情報	運用コマンド show log
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	
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
DHCP snooping バインディングデータベース	

運用コマンド backup では次に示す情報は保存しませんので注意してください。

- 運用コマンド show event-trace で表示されるイベントトレース

（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しませんので注意してください。

- 運用コマンド show log で表示される障害情報

9.3 時刻の設定と確認

9.3.1 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 9-8 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 9-9 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 9-8 Unicast モードによる時刻情報取得図（プライマリ設定時）

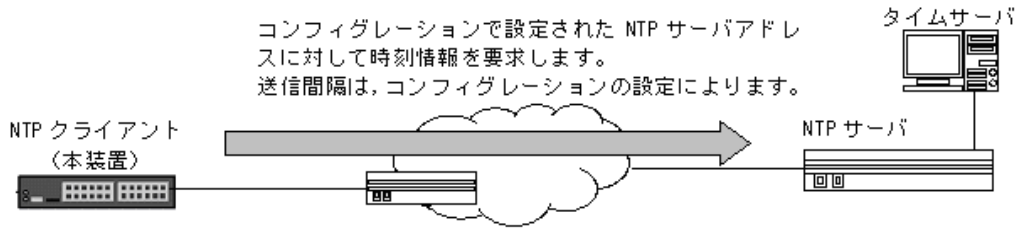
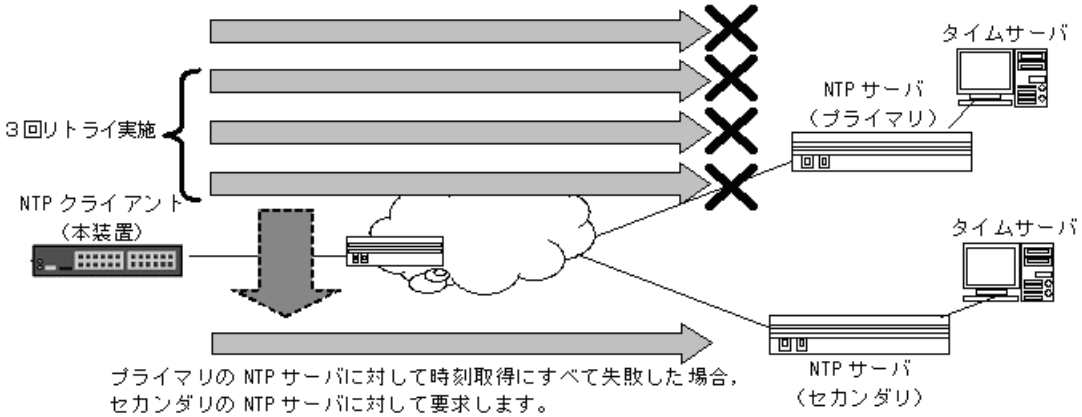


図 9-9 Unicast モードによる時刻情報取得図（プライマリ／セカンダリ設定時）



（2） マルチキャストで取得（Multicast モード）

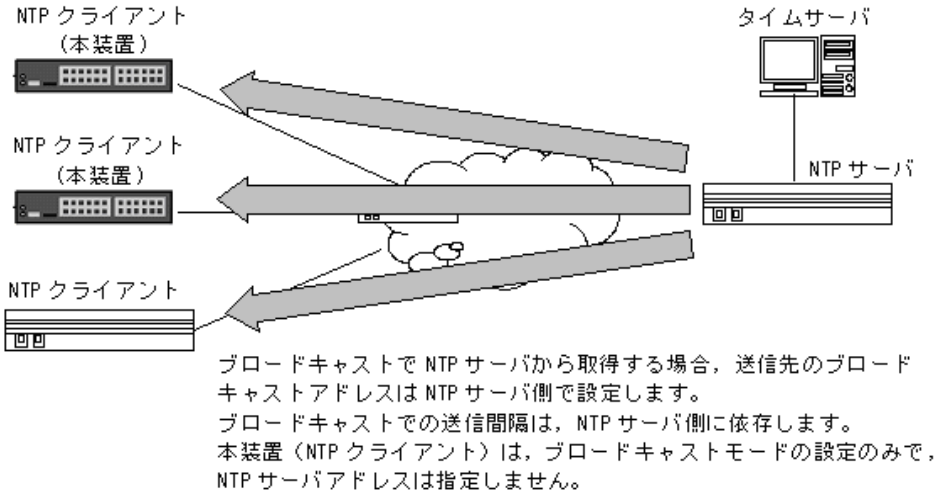
マルチキャストモードにより，NTP サーバからのマルチキャスト時刻配信を受信し，本装置内部の時計を更新します。

図 9-10 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 9-11 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。

9.3.2 コンフィグレーションコマンド・運用コマンド一覧

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

表 9-10 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。

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 9-11 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 ntp-client	NTP クライアント情報を表示します。

9.3.3 システムクロックの設定

［設定のポイント］

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

［コマンドによる設定］

1. **(config)# clock timezone JST +9**
   日本時間として，タイムゾーンに JST，UTC からのオフセットを +9 に設定します。

2. **(config)# exit**
   # copy running-config startup-config
   Do you wish to copy from running-config to startup-config? (y/n): y
   コンフィグレーションモードから装置管理者モードに移行し，保存します。

3. **# set clock 15:30:00 1 December 2006**
   2006 年 12 月 1 日 15 時 30 分に時刻を設定します。

9.3.4 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。）

10 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。

10.1　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 10-1　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。

10.2　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 10-1　ソフトウェアのアップデートの概要 (MC)

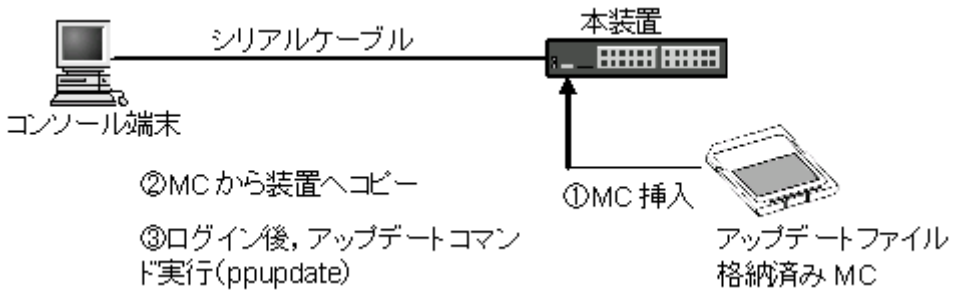
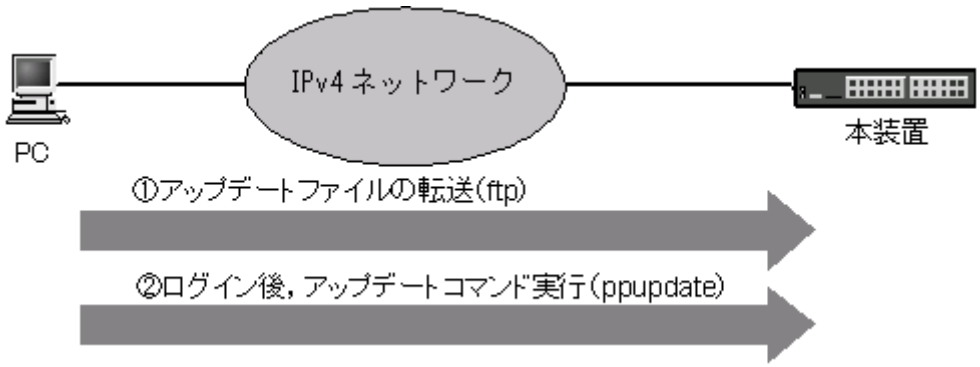


図 10-2　ソフトウェアのアップデートの概要 (ftp)



11 イーサネット

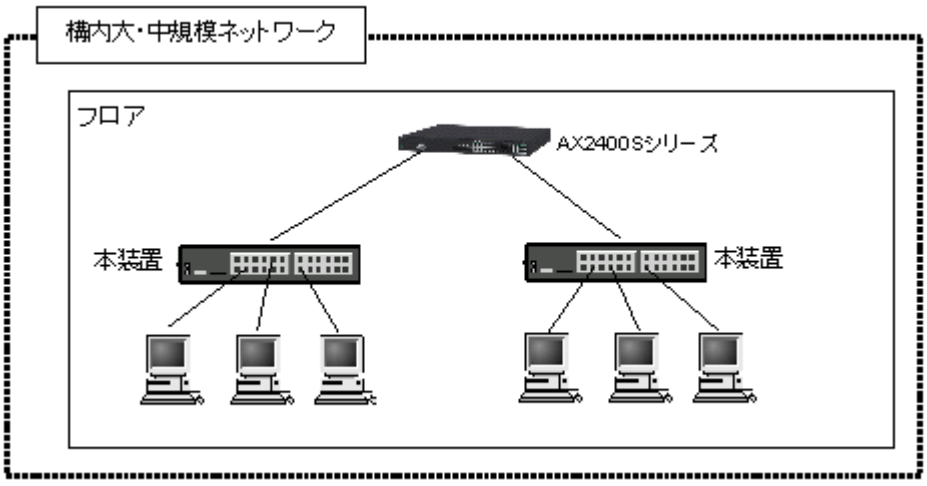
この章では，本装置のイーサネットについて説明します。

11.1 イーサネット共通の解説

11.1.1 ネットワーク構成例

本装置を使用した代表的なイーサネットの構成例を次の図に示します。ファーストイーサネットを収容しているので，フロア内の端末を 10BASE-T/100BASE-TX で接続することにより，ファーストイーサネットで十分なフロアの集線スイッチとして使用できます。

図 11-1 イーサネットの構成例



11.1.2 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。

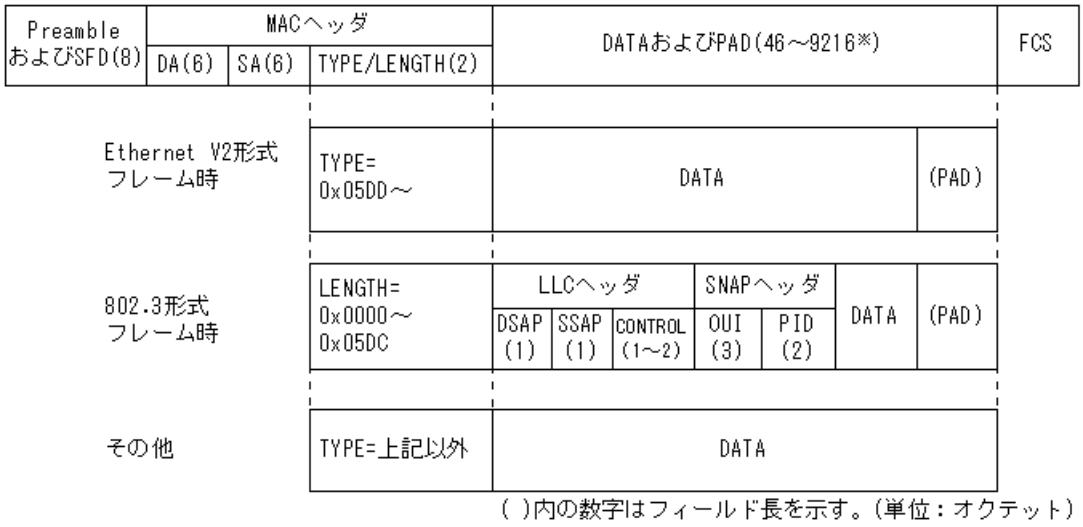
- IEEE802.3 に準拠した 10BASE-T ／ 100BASE-TX のツイストペアケーブル（UTP）を使用したインタフェース
- IEEE802.3 に準拠した 10BASE-T ／ 100BASE-TX ／ 1000BASE-T のツイストペアケーブル（UTP）を使用したインタフェース
- IEEE802.3 ※に準拠した 1000BASE-X の光ファイバを使用したインタフェース

注※
IEEE802.3ah を含みます。

11.1.3 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 11-2 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 11-1 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。

11.1.4 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 11-2 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
L2 ループ検知	装置識別子

11.1.5 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。

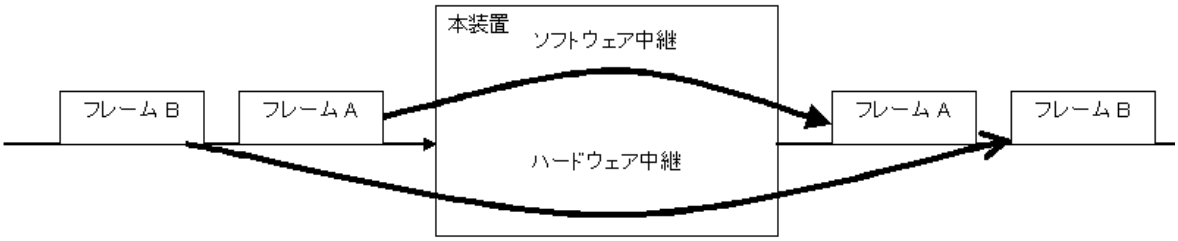
注※

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。

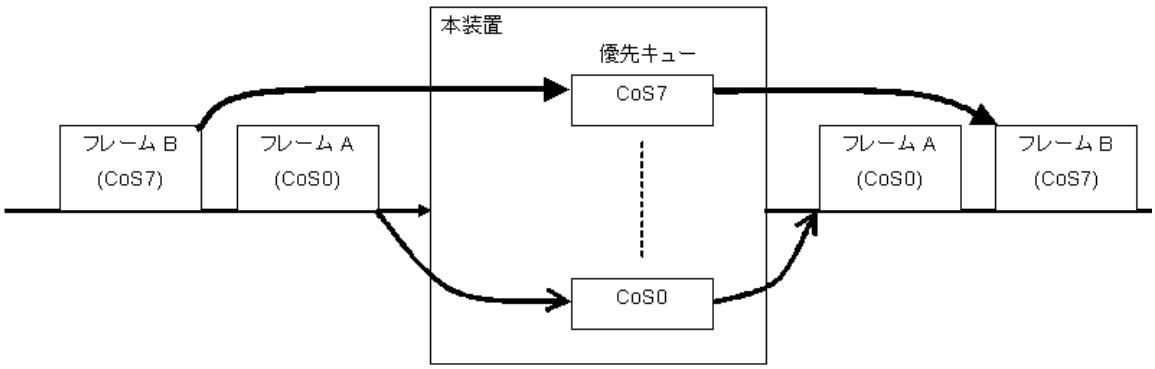
図 11-3 ソフトウェア中継によるフレームの入れ替わり



（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 11-4 優先制御によるフレームの入れ替わり



11.2 イーサネット共通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

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 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
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	10BASE-T/100BASE-TX のコンフィグレーションを設定します。
interface gigabitethernet	10BASE-T/100BASE-TX/1000BASE-T，1000BASE-X 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。
mdix auto	ポートの MDI 機能を設定します。
media-type	10BASE-T/100BASE-TX/1000BASE-T(RJ45) と 1000BASE-X(SFP) 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。

11.2.2 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。

11.2.3 イーサネットのシャットダウン

［設定のポイント］

イーサネットのコンフィグレーションでは，複数のコマンドでコンフィグレーションを設定することがあります。そのとき，コンフィグレーションの設定が完了していない状態でイーサネットがリンクアップ状態になると期待した通信ができません。従って，最初にイーサネットをシャットダウンして

から，コンフィグレーションの設定が完了したあとにイーサネットのシャットダウンを解除することを推奨します。なお，使用しないイーサネットはシャットダウンしておいてください。

［コマンドによる設定］

1. **(config)# interface 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 でイーサネッ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イーサネットが active 状態になります。イーサネットをシャットダウンした場合は，装置を再起動してもイーサネットは disable 状態のままとなり，active 状態にするためにはコンフィグレーションコマンドで 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。

11.2.4 リンクダウン検出タイマの設定

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

［設定のポイント］

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

［コマンドによる設定］

1. **(config)# interface 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。

11.2.5 AUTO-MDI/MDI-X の設定

本装置の 10BASE-T/100BASE-TX および 10BASE-T/100BASE-TX/1000BASE-T は，AUTO-MDI/MDI-X 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]

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

[コマンドによる設定]

1. **(config)# interface 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
   AUTO-MDI 機能を無効にし，MDI-X 固定にします。

11.3 イーサネット共通のオペレーション

11.3.1 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 11-4 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。
show port statistics	イーサネットの統計情報を一覧で表示します。
show port transceiver	トランシーバ情報を一覧で表示します。
clear counters	イーサネットの統計情報カウンタをクリアします。
inactivate	active 状態のイーサネットを inactive 状態にします。
activate	inactive 状態のイーサネットを active 状態にします。

11.3.2 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 11-5 「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 2006/12/14 16:47:36 UTC
Port Counts: 26
Port  Name            Status   Speed       Duplex     FCtl FrLen  ChGr/Status
 0/1  fastether0/1    up       100BASE-TX  full(auto) off   1518  -/-
 0/2  fastether0/2    up       100BASE-TX  full(auto) off   1518  -/-
 0/3  fastether0/3    down     -           -          -        -  1/up
 0/4  fastether0/4    up       100BASE-TX  full(auto) off   1518  1/up
      :
      :
```

11.4 10BASE-T/100BASE-TX の解説

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について説明します。

11.4.1 機能一覧

(1) 接続インタフェース

(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 11-5 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 11-5　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ますが，どちらか片方の設定を有効にすることで本機能が動作します。本装置と相手装置の設定内容と実行動作モードを「表 11-6　フローコントロールの送信動作」，「表 11-7　フローコントロールの受信動作」および「表 11-8　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 11-6　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 11-8　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 11-8　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 11-7　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 11-8　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 11-8　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 11-8　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
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

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
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） AUTO-MDI ／ MDI-X

AUTO-MDI ／ MDI-X 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 11-9　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，「11.1.3　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，「15.1.5　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 11-10　ジャンボフレームサポート形式

項目	フレーム形式	
	EthernetV2	IEEE802.3
中継	○	○
自装置宛	○	×

（凡例）　○：サポート　×：未サポート

表 11-11　ジャンボフレーム長

フレーム種別	Tag 無（FCS 含む）	Tag 有（FCS 含む）
ジャンボフレーム	1519 ～ 9234 バイト	1519 ～ 9238 バイト
通常フレーム	64 ～ 1518 バイト	64 ～ 1522 バイト

（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。

11.5 10BASE-T/100BASE-TX のコンフィグレーション

11.5.1 イーサネットの設定

（1） 速度と duplex の設定

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

11.5.2 フローコントロールの設定

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

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# interface 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

11.5.3 ジャンボフレームの設定

イーサネットポートでジャンボフレームを受信できるようにするためには，ポート単位の mtu を設定します。ポートの mtu の設定は，そのポートで送受信できる IPv4 パケットの最大長を指定します。本装置では，指定された mtu の IPv4 パケットに，VLAN タグが一つ付いているフレームを送受信できるようになります。

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 タグの付かないフレームであれば 8206 オクテット，VLAN タグの付いたフレームであれば 8210 オクテットまでのジャンボフレームを送受信できるようになります。

[コマンドによる設定]

1. **(config)# interface 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 タグの付かないフレームであれば 4110 オクテット，VLAN タグの付いたフレームであれば 4114 オクテットまでのジャンボフレームを送受信できるようになります。

[コマンドによる設定]

1. **(config)# system mtu 4096**

装置の全ポートの 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。

11.6 10BASE-T/100BASE-TX/1000BASE-T の解説

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

11.6.1 機能一覧

（1） 接続インタフェース

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

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

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

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

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

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

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

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

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

表 11-12 伝送速度，全二重／半二重モードごとの接続仕様

接続装置		本装置の設定				
設定	インタフェース	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 11-12　伝送速度，全二重／半二重モードごとの接続仕様」に示します。また，本装置では，ネゴシエーションで解決できなかった場合，リンク接続されるまで接続動作を繰り返します。（本動作については，「11.6.1　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 11-13　フローコントロールの送信動作」，「表 11-14　フローコントロールの受信動作」および「表 11-15　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 11-13　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 11-15　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 11-15　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 11-14　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 11-15　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 11-15　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 11-15 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
		無効	有効	on	off	行わない	行う
			無効	off	off	行わない	行わない
			desired	on	off	行わない	行う
		desired	有効	off	off	行わない	行わない
			無効	off	off	行わない	行わない
			desired	off	off	行わない	行わない

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

AUTO-MDI ／ MDI-X 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 11-16　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，「11.1.3　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，「15.1.5　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 11-17　ジャンボフレームサポート形式

項目	フレーム形式	
	EthernetV2	IEEE802.3
中継	○	○
自装置宛	○	×

（凡例）　○：サポート　×：未サポート

表 11-18　ジャンボフレーム長

フレーム種別	Tag 無（FCS 含む）	Tag 有（FCS 含む）
ジャンボフレーム	1519 ～ 9234 バイト	1519 ～ 9238 バイト
通常フレーム	64 ～ 1518 バイト	64 ～ 1522 バイト

（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 11-19　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。

11.6.2 SFP 自動認識機能 (メディアタイプの選択)

本装置の 1 ギガビットインタフェースは，10BASE-T/100BASE-TX/1000BASE-T と 1000BASE-X（SFP）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。

11.7 10BASE-T/100BASE-TX/1000BASE-T のコンフィグレーション

11.7.1 イーサネットの設定

（1） 速度と duplex の設定

本装置と相手装置の伝送速度と duplex を設定できます。デフォルトではオートネゴシエーションで，相手装置との伝送速度と 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，メディアタイプの設定については「11.7.4　メディアタイプの設定」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。

11.7.2 フローコントロールの設定

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

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

［設定のポイント］

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

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/25**
   (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

11.7.3 ジャンボフレームの設定

イーサネットポートでジャンボフレームを受信できるようにするためには，ポート単位の mtu を設定します。ポートの mtu の設定は，そのポートで送受信できる IPv4 パケットの最大長を指定します。本装置では，指定された mtu の IPv4 パケットに，VLAN タグが一つ付いているフレームを送受信できるようになります。

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 0/25 の mtu を 8192 オクテットに設定します。この設定によって，VLAN タグの付かないフレームであれば 8206 オクテット，VLAN タグの付いたフレームであれば 8210 オクテットまでのジャンボフレームを送受信できるようになります。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/25**
   (config-if)# shutdown
   (config-if)# mtu 8192

ポート 0/25 の mtu を 8192 オクテットに設定します。

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

［注意事項］

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

（2） 全ポート共通の MTU の設定

［設定のポイント］

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

［コマンドによる設定］

1. **(config)# system mtu 4096**
   装置の全ポートの 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。

11.7.4 メディアタイプの設定

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

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

11.8 1000BASE-X の解説

11.8.1 機能一覧

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

(a) 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

（b） 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 11-20　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

（2） 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 11-20　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。

（3） フローコントロール

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

本装置では，受信バッファの使用状況を監視し，相手装置の送信規制を行う場合，ポーズパケットを送信します。本装置がポーズパケット受信時は，送信規制を行います。フローコントロールのコンフィグレーションは，送信と受信でそれぞれ設定でき，有効または無効，およびネゴシエーション結果によって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 11-21　フローコントロールの送信動作」，「表 11-22　フローコントロールの受信動作」および「表 11-23　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 11-21　フローコントロールの送信動作

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

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
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 11-23　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 11-23　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 11-22　フローコントロールの受信動作

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

（凡例）

on：有効。

off：無効。desired 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 11-23　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 11-23　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 11-23　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

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

(4) 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，「11.1.3　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，「15.1.5　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 11-24 ジャンボフレームサポート形式

項目	フレーム形式	
	EthernetV2	IEEE802.3
中継	○	○
自装置宛	○	×

（凡例） ○：サポート ×：未サポート

表 11-25 ジャンボフレーム長

フレーム種別	Tag 無（FCS 含む）	Tag 有（FCS 含む）
ジャンボフレーム	1519 ～ 9234 バイト	1519 ～ 9238 バイト
通常フレーム	64 ～ 1518 バイト	64 ～ 1522 バイト

（5） SFP 自動認識機能 (メディアタイプの選択)

「11.6.2 SFP 自動認識機能 (メディアタイプの選択)」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「11.8.2 1000BASE-X 使用時の注意事項」も参照してください。

11.8.2 1000BASE-X 使用時の注意事項

（1） 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。

（2） 1000BASE-SX2 での自動メディア検出動作および制限事項

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

（3） 1000BASE-BX※の SFP 挿入時の注意事項

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

11.9 1000BASE-X のコンフィグレーション

11.9.1 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「11.7.4 メディアタイプの設定」を参照してください。

[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
   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。

11.9.2 フローコントロールの設定

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

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/25**
   (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

11.9.3 ジャンボフレームの設定

イーサネットポートでジャンボフレームを受信できるようにするためには，ポート単位の mtu を設定します。ポートの mtu の設定には，そのポートで送受信できる IPv4 パケットの最大長を指定します。本装置では，指定された mtu の IPv4 パケットに，VLAN タグが一つ付いているフレームを送受信できるようになります。

[設定のポイント]

ポートの mtu の設定値は，ネットワークおよび相手装置と合わせて決定します。
ここでは，ポートの mtu を 8192 オクテットに設定します。この設定によって，VLAN タグの付かないフレームであれば 8206 オクテット，VLAN タグの付いたフレームであれば 8210 オクテットまでのジャンボフレームを送受信できるようになります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/25**
(config-if)# shutdown
ポート 0/25 をシャットダウンします。

2. **(config-if)# mtu 8192**
ポート 0/25 の mtu を 8192 オクテットに設定します。

3. **(config-if)# no shutdown**
(config-if)# exit
ポート 0/25 のシャットダウンを解除します。

11.9.4 メディアタイプの設定

「11.7.4 メディアタイプの設定」を参照してください。

11.10 PoE の解説

11.10.1 PoE の概要

PoE(Power over Ethernet) とは，データ通信用の RJ45 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。最小 4.0W から最大 15.4W 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 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 Pre.STD や IEEE802.3af 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 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 規定の電流を消費する動作をすることから，本装置は四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 Class1 ～ Class3 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 Class0 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 11-26　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 11-26　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

11.10.2 PoE の仕様

(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 11-27　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		AX1230S-24P2C AX1230S-24P2CA
本装置の PoE 供給電力		170.0W
PoE 供給可能ポート※1	Class 0 の場合	11 ～ 24 ポート※2※3
	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	11 ポート

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

15.4W を消費する受電装置の最大接続可能数は 11 ポートとなります。（15.4W × 11 ＝ 169.4W）

注※ 3

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。

（2） PoE 供給電力の割り当て

PoE 供給電力（ポートに割り当てる電力の総和）は 170.0W 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）≧

Class0 のポート数×出力電力（15.4W）＋

Class1 のポート数×出力電力（4.0W）＋

Class2 のポート数×出力電力（7.0W）＋

Class3 のポート数×出力電力（15.4W）

Class0 機器については実際の消費電力が分からないため，15.4W で計算することをお奨めします。

（3） PoE の給電停止について

受電装置への供給電力の総和が計算上 170W 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 170W 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（170W）＜

Class0 機器への実出力電力の総和※＋

Class1 のポート数×出力電力（4.0W）＋

Class2 のポート数×出力電力（7.0W）＋

Class3 のポート数×出力電力（15.4W）

注※

Class0 機器については消費電力値が判定できないため実出力電力の総和で監視します。従って

Class0 機器を接続している場合で，Class0 機器への出力電力の経時的な変動が発生すると，優先度の低いポートへの電力供給を停止する可能性があります。

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。）

（4） 電力供給の優先度

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，ポート内で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。

本機能には，次の設定があります。

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。

11.11 PoE のコンフィグレーション

11.11.1 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 11-28 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	ポートの PoE 機能を設定します。

11.11.2 PoE 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
   (config-if)# exit
   PoE 機能で電力を供給しないように設定します。

11.12 PoE のオペレーション

11.12.1 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 11-29 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。

11.12.2 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，PoEStatus に「on」を表示し，さらに Class に IEEE802.3af 準拠電力クラス，Cur/Vol/Power にポート単位の電流 / 電圧 / 消費電力状態を表示します。

運用コマンド show power inline の実行結果を次の図に示します。

図 11-6 「PoE 電力供給状態」の表示例

```
> show power inline

Date 2007/6/21 12:00:00 UTC
Threshold(W): 170
Allocate(W) :  34
Port Counts: 24
 Port  Name           PoEStatus  Class  Priority  Cur(mA)  Vol(V)  Power(mW)
 0/1   fastether0/1   on         0      high          108    49.3       5324
 0/2   fastether0/2   on         0      high          101    49.3       4979
 0/3   fastether0/3   on         0      high          101    49.3       4979
       :
       :
>
```

12 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。

12.1　リンクアグリゲーション基本機能の解説

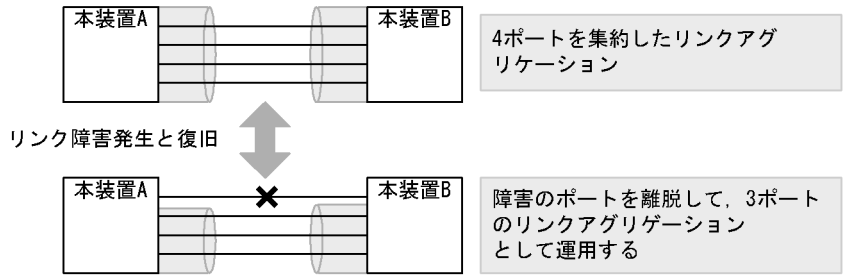
12.1.1　概要

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。

12.1.2　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 12-1　リンクアグリゲーションの構成例



12.1.3　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 12-1　リンクアグリゲーションのサポート仕様

項目	サポート仕様	備考
装置当たりのリンクアグリゲーショングループ数	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。

12.1.4　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。

12.1.5　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 12-2　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

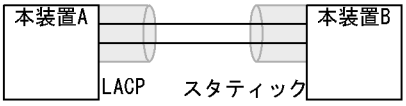
12.1.6　リンクアグリゲーション使用時の注意事項

（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。

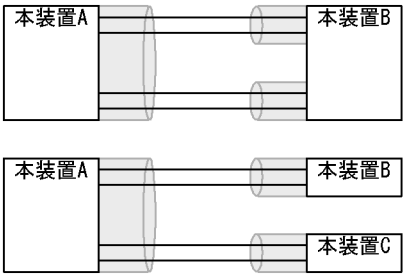
図 12-2 リンクアグリゲーションが不可能な構成例

●装置間でモードが異なる場合



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

●装置間でチャネルグループがポイントーマルチポイントになっている場合



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

(2) リンクアグリゲーションの設定手順

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

(3) CPU 過負荷時

LACP リンクアグリゲーションモード使用時に CPU が過負荷な状態になった場合，本装置が送受信する LACPDU の廃棄または処理遅延が発生して，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。

(4) チャネルグループ内のポートに障害が発生したとき

- 【Ver.1.4.A まで】
  チャネルグループ内の最若番のポートに障害が発生すると，チャネルグループはいったんダウンします。
- 【Ver.1.4.B 以降】
  上記制限は解除されています。

12.2 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

12.2.1 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 12-3 コンフィグレーションコマンド一覧

コマンド名	説明
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。

12.2.2 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。

12.2.3 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。

12.2.4 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 12-4 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
L2 ループ検知	loop-detection

(2) チャネルグループ上で動作する機能の設定

[設定のポイント]

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

［コマンドによる設定］

1. **(config)# interface range 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。

12.2.5 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 12-4　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 12-4　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。

12.3　リンクアグリゲーション拡張機能の解説

12.3.1　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。

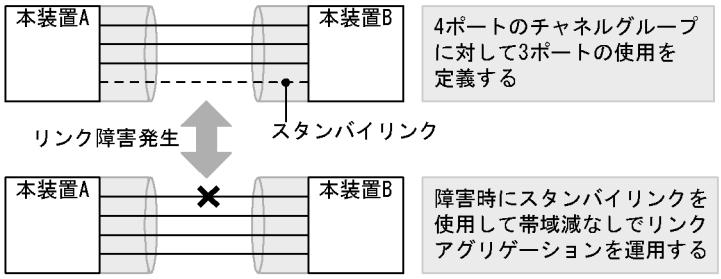
待機用ポートは，コンフィグレーションで設定するポート優先度，ポート番号から選択されます。待機用ポートは，次の表に示すように選択優先度の高い順に決定します。

表 12-5　待機用ポートの選択方法

選択優先度	パラメータ	備考
高 ↑ ↓ 低	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
	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 12-3　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。Ver.1.4.A までと Ver.1.4.B 以降では，若干動作が異なります。

（a）Ver.1.4.A までの動作

1. 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。
2. 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。

（b） Ver.1.4.B 以降の動作

1. 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。
2. 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。

運用中のポートが一つのときの動作：

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。）

12.4　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

12.4.1　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 12-6　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。

12.4.2　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。

12.5 リンクアグリゲーションのオペレーション

12.5.1 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 12-7 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。

12.5.2 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 12-4 show channel-group の実行結果

```
> show channel-group channel-group-number 7

Date 2006/12/12 19:58:06 UTC
ChGr: 7   Mode: LACP
  CH Status     : Down    Elapsed Time: -
  MAC address   : -
  Actor System  : Priority: 128    MAC: 00ee.f214.0001  Key: 7
  Partner System: Priority: 128    MAC: 0012.e228.b3b4  Key: 1
  Port Information
    0/18  Up    State: Attached
    0/21  Up    State: Detached
    0/24  Up    State: Detached
>
```

(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 12-5 show channel-group detail の実行結果

```
> show channel-group detail

Date 2006/12/13 22:23:53 UTC
ChGr: 7   Mode: LACP
  CH Status     : Up      Elapsed Time: 00:14:04
  MAC address   : 00ee.f214.0112
  Actor System  : Priority: 128    MAC: 00ee.f214.0001  Key: 7
  Partner System: Priority: 128    MAC: 0012.e228.b3b4  Key: 2
  Port Information
  Port: 0/18  Up    State: Distributing  Speed: 100M   Duplex: Full
    Actor   Port  : Priority: 128
    Partner System: Priority: 128    MAC: 0012.e228.b3b4  Key: 2
    Partner Port  : Priority: 128    Number: 44
  Port: 0/21  Up    State: Distributing  Speed: 100M   Duplex: Full
    Actor   Port  : Priority: 128
    Partner System: Priority: 128    MAC: 0012.e228.b3b4  Key: 2
    Partner Port  : Priority: 128    Number: 45
  Port: 0/24  Up    State: Distributing  Speed: 100M   Duplex: Full
    Actor   Port  : Priority: 128
    Partner System: Priority: 128    MAC: 0012.e228.b3b4  Key: 2
    Partner Port  : Priority: 128    Number: 46
>
```

13 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。

13.1　概要

13.1.1　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。

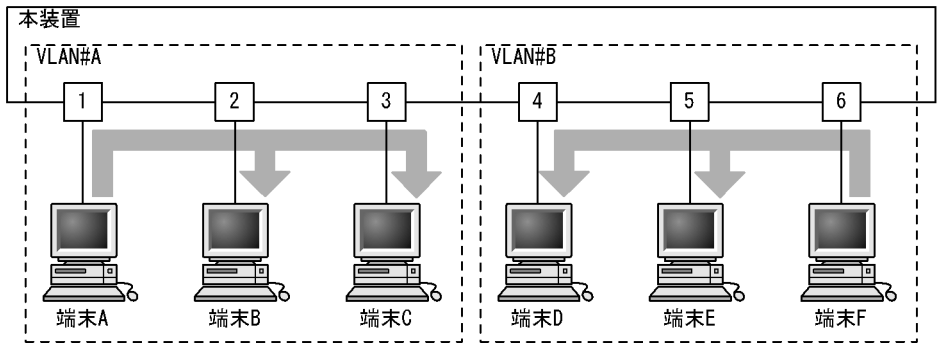
レイヤ 2 スイッチは，MAC アドレステーブルのエントリに従ってフレームを中継します。フレームの宛先 MAC アドレスに一致するエントリがあると，そのエントリのポートに中継します（エントリのポートが受信したポートである場合は中継しません）。一致するエントリがない場合，受信したポート以外のすべてのポートにフレームを中継します。この中継をフラッディングと呼びます。

13.1.2　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 13-1　VLAN の概要



13.2　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 13-1　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
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

13.3　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 13-2　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	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+	
		ポートミラーリング (ミラーポート)	
	MAC VLAN	デフォルト VLAN	共存不可
		PVST+	
		ポートミラーリング (ミラーポート)	
デフォルト VLAN		プロトコル VLAN	共存不可
		MAC VLAN	
		IGMP snooping	
		MLD snooping	
		ポートミラーリング (ミラーポート)	
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)	IEEE802.1X ポート単位認証	共存不可
		IEEE802.1X VLAN 単位認証 (動的)	

VLAN とレイヤ 2 認証機能の動作については，マニュアル「コンフィグレーションガイド Vol.2」の各認証機能の解説を参照してください。

表 13-3　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	
	IEEE802.1X	一部制限あり※
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	
	IEEE802.1X	一部制限あり※
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	

使用したい機能	制限のある機能	制限の内容
	PVST+	
	ループガード	
	IEEE802.1X	一部制限あり※

注※

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

表 13-4 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
	リンクアグリゲーション	
MLD snooping	デフォルト VLAN	共存不可
	リンクアグリゲーション	

14 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。

14.1 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。

14.1.1 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。

14.1.2 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。

14.1.3 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 14-1 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。

14.1.4 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 14-2 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。

14.1.5 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 14-3　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. 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 2. 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

14.2　MAC アドレス学習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

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 14-4　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。

14.2.2　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，「14.1.5　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。

14.2.3　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］

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

は廃棄します。

(2) 出力先にリンクアグリゲーションを指定するスタティックエントリ

[設定のポイント]

出力先にリンクアグリゲーションを指定した例を示します。

[コマンドによる設定]

1. **(config)# mac-address-table static 0012.e200.1122 vlan 10 interface port-channel 5**

   VLAN 10 で，宛先 MAC アドレス 0012.e200.1122 のフレームの出力先をチャネルグループ 5 に設定します。

[注意事項]

VLAN 10 で，送信元 MAC アドレス 0012.e200.1122 のフレームをチャネルグループ 5 以外から受信した場合は廃棄します。

14.3　MAC アドレス学習のオペレーション

14.3.1　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 14-5　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。

14.3.2　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 14-1　show mac-address-table の実行結果

```
> show mac-address-table

Date 2008/05/30 14:44:52 UTC
Aging time : 300
No    MAC address      VLAN    Type    Port     ChGrp    MCast
1     00b0.d0ad.8df7     10    MacAuth 0/7      -        -
2     0000.87de.2948     10    Dynamic 0/19     -        -
2     0000.87de.2948     10    Dynamic 0/19     -        -
4     0013.20a5.2d9f    100    MacAuth 0/9      -        -
5     0000.87de.29c8    100    Dynamic 0/21     -        -
6     000a.e426.9656    100    Dynamic 0/5      -        -
7     0000.0000.0001   4094    Dynamic 0/9      -        -
8     0000.0088.7701   4094    Dynamic 0/23     -        -
       :
       :

>
```

14.3.3　MAC アドレス学習数の確認

運用コマンド show mac-address-table（learning-counter パラメータ）で MAC アドレス学習によって登録したダイナミックエントリの数をポート単位に表示できます。このコマンドで，ポートごとの接続端末数の状態を確認できます。

リンクアグリゲーションを使用している場合，同じチャネルグループのポートはすべて同じ値を表示します。表示する値はチャネルグループ上で学習したアドレス数です。

図 14-2 show mac-address-table（learning-counter パラメータ指定）の実行結果

```
> show mac-address-table learning-counter port 0/5

Date 2006/12/13 22:57:55 UTC
Port          Count
0/5            1051

>
```

15 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。

15.1 VLAN 基本機能の解説

この節では，VLAN の概要を説明します。

15.1.1 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 15-1 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。

15.1.2 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 15-2 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「15.7.4 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 15-3 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。

15.1.3 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。

15.1.4 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。

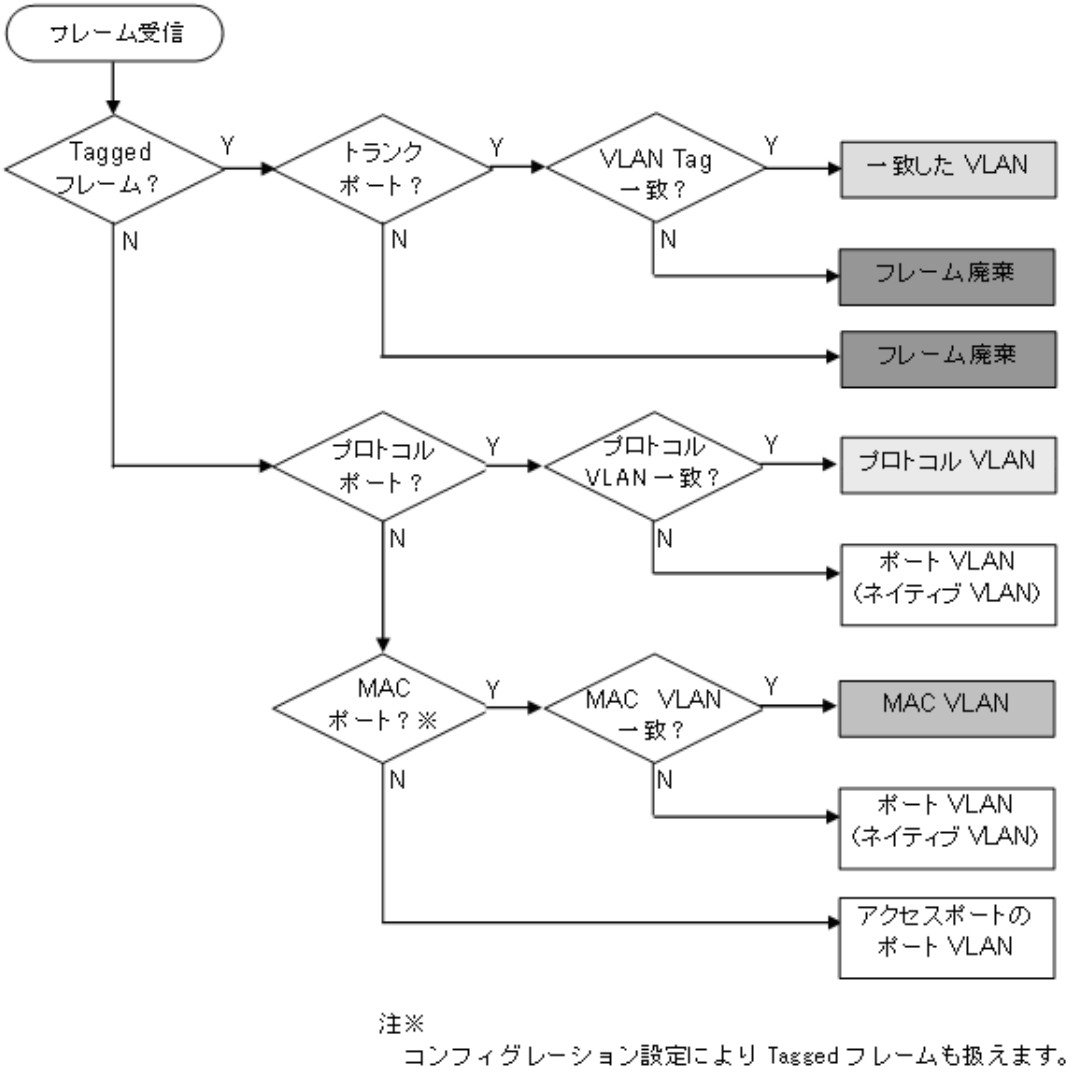
表 15-4　VLAN 判定の優先順位

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「15.7.4　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 15-1　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。

15.1.5 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。

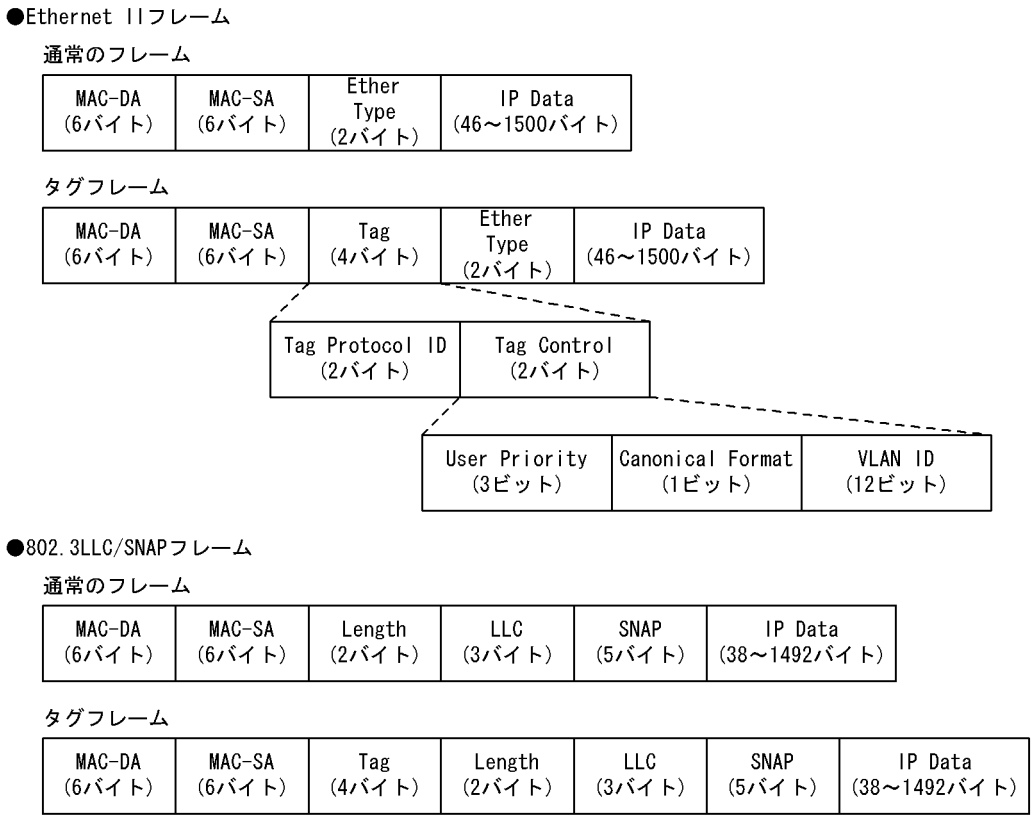
VLAN Tag はトランクポート，MAC ポートで使用します。トランクポート，MAC ポートはその対向装置も VLAN Tag を認識できなければなりません。

（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。

VLAN Tag 付きフレームのフォーマットを次の図に示します。VLAN Tag を挿入するイーサネットフレームのフォーマットは，Ethernet V2 フォーマットと 802.3 フォーマットの 2 種類があります。

図 15-2 VLAN Tag 付きフレームのフォーマット



VLAN Tag のフィールドの説明を次の表に示します。

表 15-5 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。
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」

15.1.6 VLAN 使用時の注意事項

(1) ミラーポートに関する注意事項

ミラーポートを設定したポートは VLAN のポートとしては使用できません。

15.2 VLAN 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

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 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
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。

15.2.2 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。

15.2.3 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。

15.2.4 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，「15.4.3　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。

15.3 ポート VLAN の解説

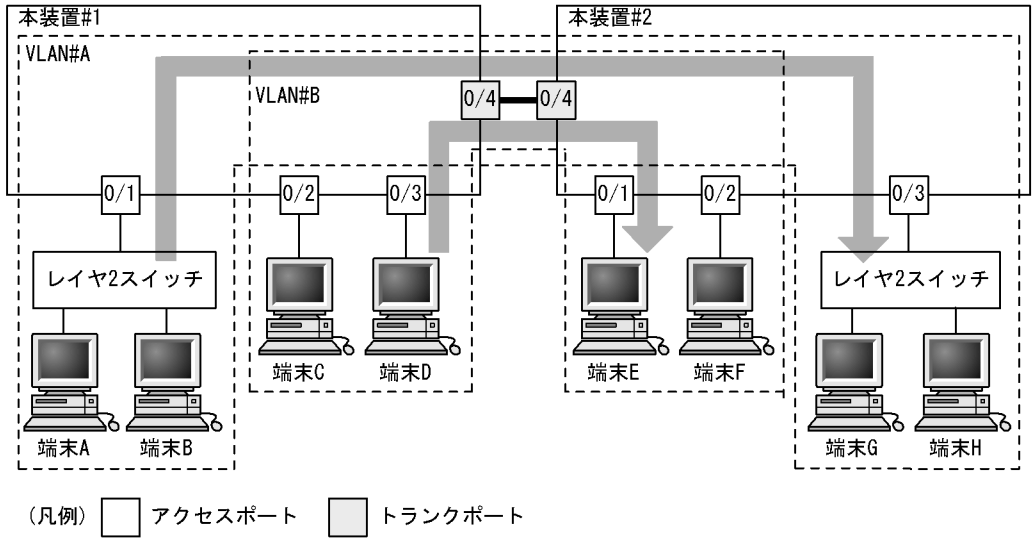
ポート単位に VLAN のグループ分けを行います。

15.3.1 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 15-3 ポート VLAN の構成例



トランクポートは複数のVLANを設定することができます。
トランクポートではVLAN Tagを付与して中継することでVLANを識別します。

15.3.2 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 15-3 ポート VLAN の構成例」のトランクポートにおいて VLAN#B をネイティブ VLAN に設定すると，VLAN#B はトランクポートでも Untagged フレームで中継します。

15.3.3 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。

15.4 ポート VLAN 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

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 15-7 コンフィグレーションコマンド一覧

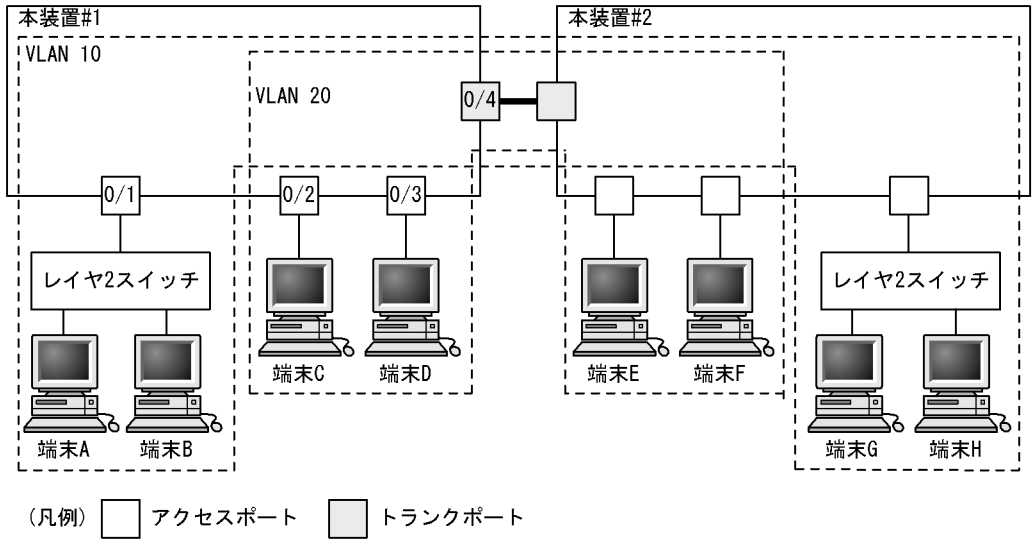
コマンド名	説明
switchport access	アクセスポートの VLAN を設定します。
switchport mode	ポートの種類（アクセス，トランク）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan	ポート VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。

15.4.2 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 15-4 ポート VLAN の設定例



(1) ポート VLAN の作成

[設定のポイント]

ポート VLAN を作成します。VLAN を作成する際に VLAN ID だけを指定して VLAN の種類を指定しないで作成するとポート VLAN となります。

[コマンドによる設定]

1. **(config)# vlan 10,20**
   (config-vlan)# exit

VLAN ID 10，VLAN ID 20 をポート VLAN として作成します。

（2） アクセスポートの設定

一つのポートに一つの VLAN を設定して Untagged フレームを扱う場合，アクセスポートとして設定します。

［設定のポイント］

ポートをアクセスポートに設定して，そのアクセスポートで扱う VLAN を設定します。

［コマンドによる設定］

1. **(config)# interface 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。

15.4.3 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。

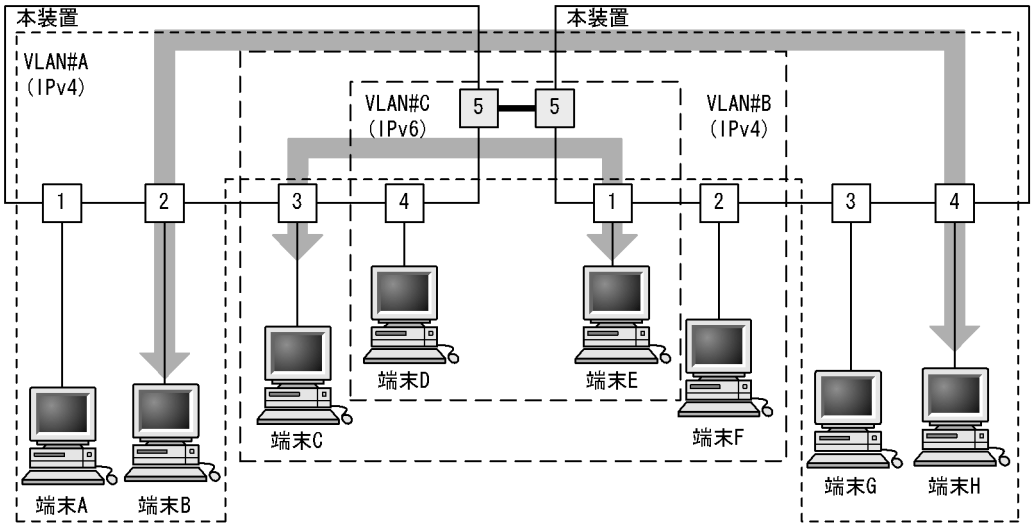
15.5 プロトコル VLAN の解説

15.5.1 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 15-5 プロトコル VLAN の構成例



・VLAN#A，#BはIPv4プロトコルのVLANです。
・VLAN#CはIPv6プロトコルのVLANです。
・端末D，EはVLAN#B，#Cの両方に属しています。
・矢印は端末Bと端末H間，端末Cと端末E間で同じVLANで通信している例です。

15.5.2 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 15-8 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。

15.5.3 プロトコルポートとトランクポート

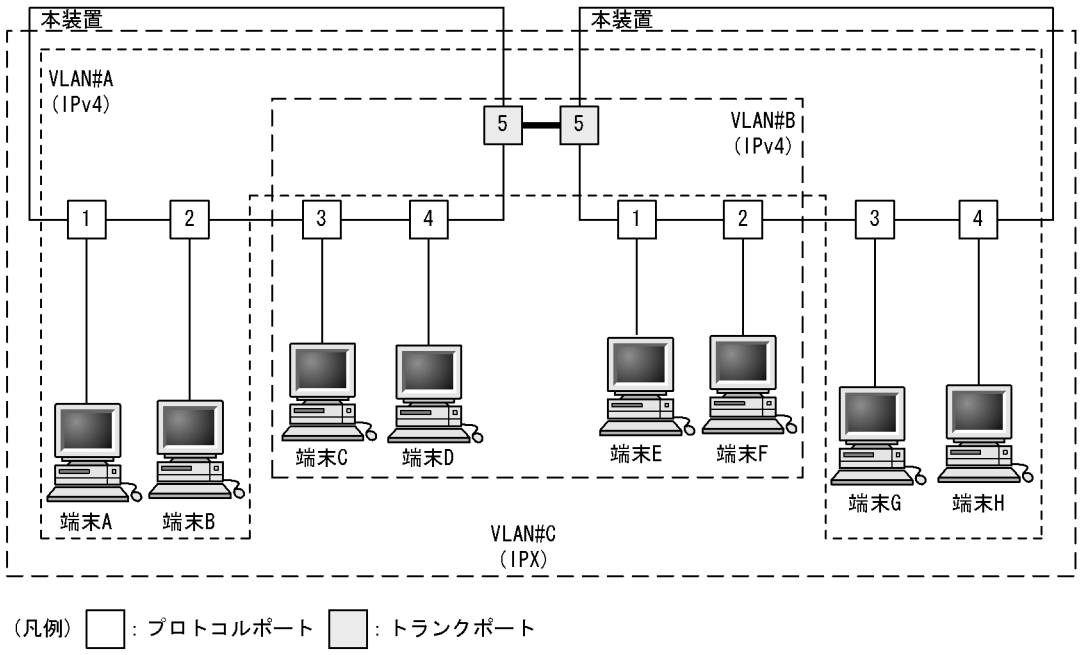
プロトコルポートは Untagged フレームのプロトコルを識別します。プロトコル VLAN として使用するポートはプロトコルポートを設定します。プロトコルポートには複数のプロトコルで異なる VLAN を割り当てることもできます。複数のプロトコル VLAN をほかの LAN スイッチなどに接続するためにはトランクポートを使用します。なお，トランクポートは VLAN Tag によって VLAN を識別するため，プロトコルによる識別は行いません。

15.5.4 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 15-6 プロトコルポートでネイティブ VLAN を使用する構成例



・VLAN#A，#Bはポート VLANでネイティブVLANとして設定します。
・VLAN#CはIPXプロトコルのVLANです。
・すべての端末はIPXプロトコルVLANに属しています。
・端末A，B，G，Hと端末C，D，E，Fはそれぞれ異なるポートVLANに属しています。

15.6 プロトコル VLAN のコンフィグレーション

15.6.1 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 15-9 コンフィグレーションコマンド一覧

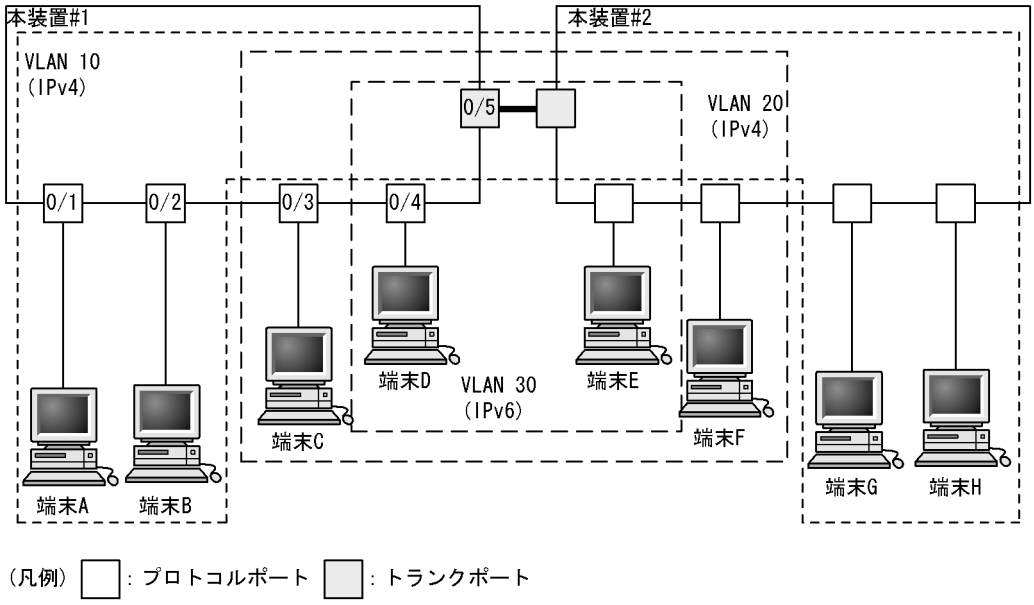
コマンド名	説明
protocol	プロトコル VLAN で VLAN を識別するプロトコルを設定します。
switchport mode	ポートの種類（プロトコル，トランク）を設定します。
switchport protocol	プロトコルポートの VLAN を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan-protocol	プロトコル VLAN 用のプロトコル名称とプロトコル値を設定します。
vlan protocol-based	プロトコル VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。

15.6.2 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 15-7 プロトコル VLAN の設定例



(1) VLAN を識別するプロトコルの作成

［設定のポイント］

プロトコル VLAN は，VLAN を作成する前に識別するプロトコルを vlan-protocol コマンドで設定します。プロトコルは，プロトコル名称とプロトコル値を設定します。一つの名称に複数のプロトコル値を関連づけることもできます。
IPv4 プロトコルは，IPv4 の EtherType 値と同時に ARP の EtherType 値も指定する必要があるため，IPv4 には二つのプロトコル値を関連づけます。

［コマンドによる設定］

1. **(config)# vlan-protocol IPV4 ethertype 0800,0806**
   名称 IPV4 のプロトコルを作成します。プロトコル値として，IPv4 の EtherType 値 0800 と ARP の EtherType 値 0806 を関連づけます。
   なお，この設定でのプロトコル判定は EthernetV2 形式のフレームだけとなります。

2. **(config)# vlan-protocol IPV6 ethertype 86dd**
   名称 IPV6 のプロトコルを作成します。プロトコル値として IPv6 の EtherType 値 86DD を関連づけます。

［注意事項］
EtherType 値は，05FF 以下の値の場合，0000 で動作します。

（2） プロトコル VLAN の作成

［設定のポイント］
プロトコル VLAN を作成します。VLAN を作成する際に VLAN ID と protocol-based パラメータを指定します。また，VLAN を識別するプロトコルとして，作成したプロトコルを指定します。

［コマンドによる設定］

1. **(config)# vlan 10,20 protocol-based**
   VLAN 10，20 をプロトコル VLAN として作成します。VLAN 10，20 は同じ IPv4 プロトコル VLAN とするため一括して設定します。本コマンドで VLAN コンフィグレーションモードに移行します。

2. **(config-vlan)# protocol IPV4**
   (config-vlan)# exit
   VLAN 10，20 を識別するプロトコルとして，作成した IPv4 プロトコルを設定します。

3. **(config)# vlan 30 protocol-based**
   (config-vlan)# protocol IPV6
   (config-vlan)# exit
   VLAN 30 をプロトコル VLAN として作成します。また，VLAN 30 を識別するプロトコルとして，作成した IPv6 プロトコルを設定します。

（3） プロトコルポートの設定

［設定のポイント］
プロトコル VLAN でプロトコルによって VLAN を識別するポートは，プロトコルポートを設定します。このポートでは Untagged フレームを扱います。

［コマンドによる設定］

1. **(config)# interface 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]

switchport protocol vlan コマンドは，それ以前のコンフィグレーションに追加するコマンドではなく指定した <VLAN ID list> に設定を置き換えます。すでにプロトコル VLAN を運用中のポートで VLAN の追加や削除を行う場合は, switchport protocol vlan add コマンドおよび switchport protocol vlan remove コマンドを使用してください。

（4） トランクポートの設定

[設定のポイント]

プロトコル VLAN においても，Tagged フレームを扱うポートはトランクポートとして設定し，そのトランクポートに VLAN を設定します。

[コマンドによる設定]

1. **(config)# interface 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。

15.6.3 プロトコルポートのネイティブ VLAN の設定

[設定のポイント]

プロトコルポートで設定したプロトコルに一致しない Untagged フレームを扱いたい場合，そのフ

レームを扱うVLANとしてネイティブVLANを設定します。ネイティブVLANはポートVLANだけが設定できます。
ネイティブVLANのVLAN IDをswitchport protocol native vlanコマンドで設定すると，プロトコルポート上で設定したプロトコルに一致しないUntaggedフレームを扱うVLANとなります。ネイティブVLANは，コンフィグレーションで明示して設定しない場合はVLAN 1（デフォルトVLAN）です。
ネイティブVLANにstatus suspendが設定されている場合は，設定したプロトコルと一致しないフレームが中継されません。

［コマンドによる設定］

1. **(config)# vlan 10,20 protocol-based**
   (config-vlan)# exit
   (config)# vlan 30
   (config-vlan)# exit
   VLAN 10，20をプロトコルVLANとして作成します。また，VLAN 30をポートVLANとして作成します。

2. **(config)# interface 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。

15.7 MAC VLAN の解説

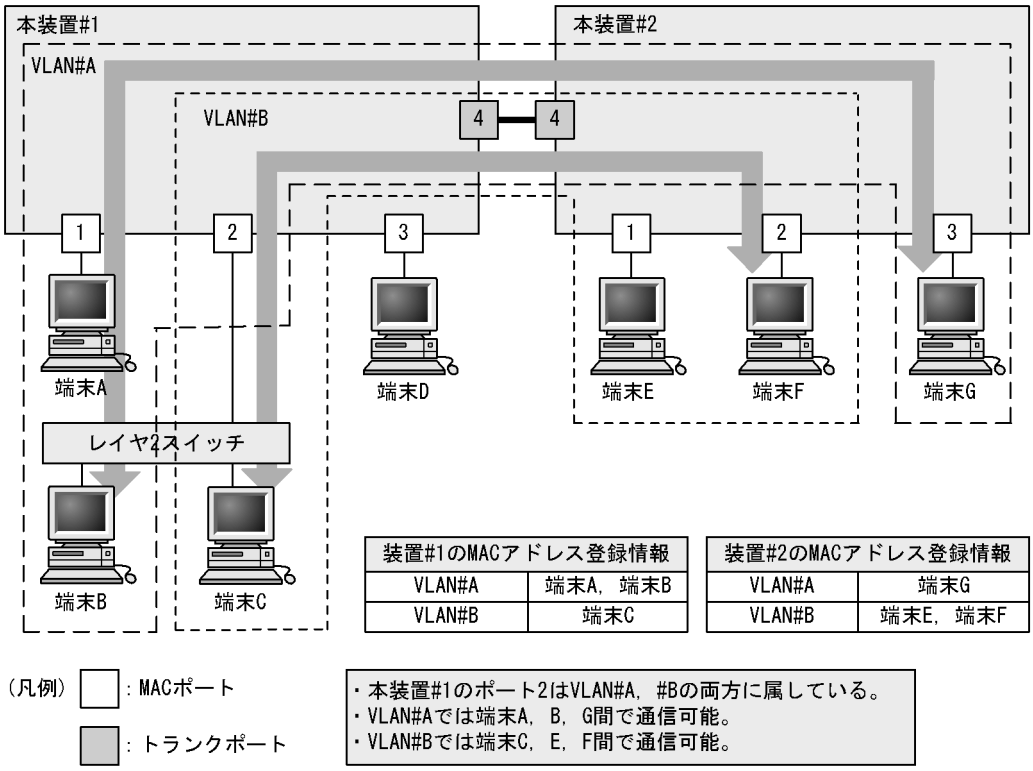
15.7.1 概要

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 15-8　MAC VLAN の構成例



15.7.2 装置間の接続と MAC アドレス設定

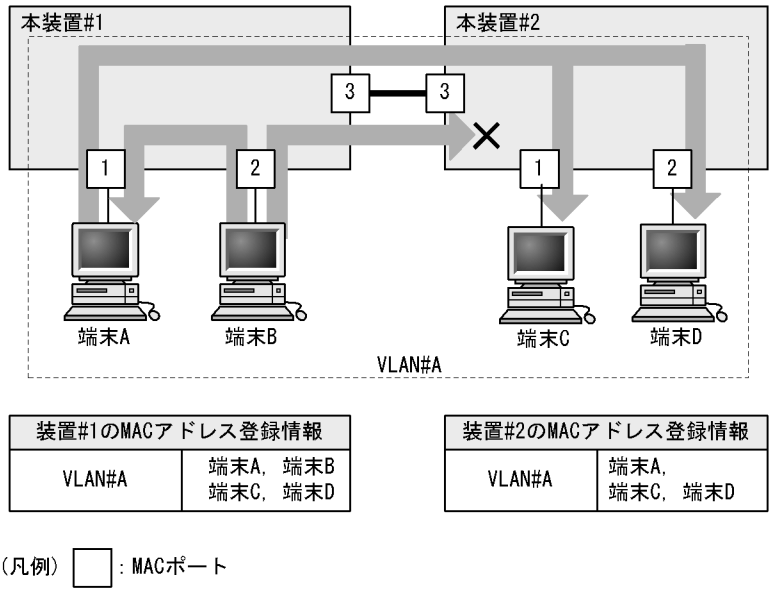
複数の装置で MAC VLAN を構成する場合，装置間の接続はトランクポートをお勧めします。トランクポートで受信したフレームの VLAN 判定は VLAN Tag で行います。そのため，送信元 MAC アドレスが VLAN に設定されていなくても，MAC VLAN で通信できます。トランクポートで装置間を接続した場合については，「図 15-8　MAC VLAN の構成例」を参照してください。

MAC ポートで装置間を接続する場合は，その VLAN に属するすべての MAC アドレスをすべての装置に設定する必要があります。ルータが存在する場合は，ルータの MAC アドレスも登録してください。また，

VRRP を使用している場合は，仮想ルータ MAC アドレスを登録してください。

MAC ポートで装置間を接続した場合の図を次に示します。

図 15-9　装置間を MAC ポートで接続した場合



・端末Aは，本装置#1，#2の両方に設定があるため，端末C，端末Dと通信可能。
・端末Bは，本装置#2に設定がないため，端末C，端末Dと通信不可。
　端末Aとは通信可能。

15.7.3　レイヤ 2 認証機能との連携について

MAC VLAN は，レイヤ 2 認証機能と連携して，VLAN への MAC アドレスを動的に登録できます。連携するレイヤ 2 認証機能を次に示します。

- IEEE802.1X：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「15.7.4 MAC ポートのオプション機能」を参照してください。

15.7.4 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 15-11　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 15-10　中継先と Tagged フレームの処理

中継先	Tagged フレームの処理
アクセスポート	Tag を外して Untagged フレームを送信
トランクポートのネイティブ VLAN	Tag を外して Untagged フレームを送信
トランクポートのネイティブ VLAN 以外	Tagged フレームを送信
プロトコルポートのネイティブ VLAN	Tag を外して Untagged フレームを送信
MAC ポートの MAC VLAN	Tag を外して Untagged フレームを送信
MAC ポートの dot1q vlan で指定した VLAN	Tagged フレームを送信

(3) オプション機能使用時の注意事項

(a) VLAN の排他について

下記のコンフィグレーションコマンドで指定する VLAN は，すべて排他設定となります。いずれかに設定した VLAN ID を，その他のコマンドで設定することはできません。

表 15-11　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
  「15.7.3　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 15-11　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。

15.8 MAC VLAN のコンフィグレーション

15.8.1 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 15-12 コンフィグレーションコマンド一覧

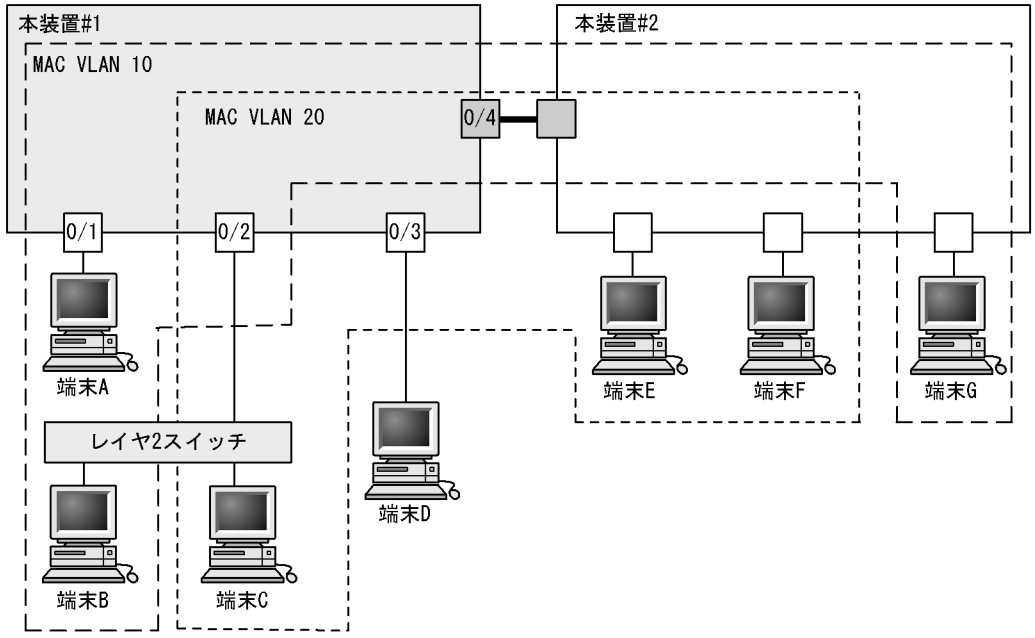
コマンド名	説明
mac-address	MAC VLAN で VLAN に所属する端末の MAC アドレスをコンフィグレーションによって設定します。
switchport mac-vlan	MAC ポートの VLAN を設定します。
switchport mode	ポートの種類（MAC，トランク）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan mac-based	MAC VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。

15.8.2 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 15-10　MAC VLAN の設定例



装置#1のMACアドレス登録情報		
VLAN 10	端末A	0012.e200.0001
	端末B	0012.e200.0002
VLAN 20	端末C	0012.e200.0003

（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。

15.8.3 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。

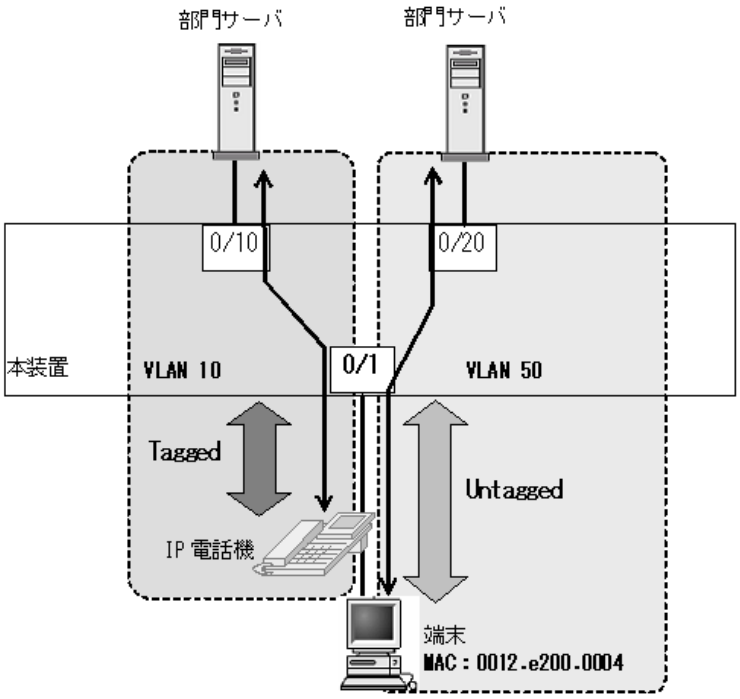
15.8.4 MAC ポートでの Tagged フレーム中継の設定

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 15-11　MAC ポートでの Tagged フレーム中継の設定例



［設定のポイント］

MAC ポートを設定し，同一 MAC ポートで Tagged フレームと Untagged フレームを扱うポートとして設定します。また，MAC VLAN には端末の MAC アドレスを設定します。

- VLAN 10：ポート VLAN で Tagged フレームを扱います。
- VLAN 50：MAC VLAN で Untagged フレームを扱います。

［コマンドによる設定］

1. **(config)# vlan 10**
   (config-vlan)# exit
   VLAN 10 をポート VLAN として作成します。

2. **(config)# vlan 50 mac-based**
   (config-vlan)# mac-address 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。）

15.9 VLAN のオペレーション

15.9.1 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 15-13 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。

15.9.2 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 15-12　show vlan の実行結果

```
> show vlan

Date 2008/03/13 13:12:20 UTC
VLAN counts: 9
VLAN ID: 1     Type: Port based  Status: Up
  Learning: On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0001
  IP Address:
  Source MAC address: 00ee.f090.0001(System)
  Description: VLAN0001
  Spanning Tree: MSTP(802.1S)
  IGMP snooping:      MLD snooping:
  Untagged(9)    : 0/1,0/7-11,0/17-18,0/21
  Tagged(4)      : 0/4,0/14,0/24,0/26
VLAN ID: 2     Type: Protocol based  Status: Up
  Protocol VLAN Information  Name: "vlan2"
  EtherType:  LLC:  Snap-EtherType:
  Learning: On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0002
  IP Address:
  Source MAC address: 00ee.f090.0001(System)
  Description: VLAN0002
  Spanning Tree: MSTP(802.1S)
  IGMP snooping:      MLD snooping:
  Untagged(4)    : 0/6,0/16,0/19,0/25
  Tagged(4)      : 0/4,0/14,0/24,0/26
VLAN ID: 3     Type: MAC based  Status: Up
  Learning: On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0003
  IP Address:
  Source MAC address: 00ee.f090.0001(System)
  Description: VLAN0003
  Spanning Tree: MSTP(802.1S)
  IGMP snooping:      MLD snooping:
  Untagged(3)    : 0/5,0/15,0/20
  Tagged(4)      : 0/4,0/14,0/24,0/26
             :
             :
>
```

（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 15-13　show vlan detail の実行結果

```
> show vlan id 2000 detail

Date 2008/03/13 13:13:36 UTC
VLAN counts: 1
VLAN ID: 2000  Type: Protocol based  Status: Up
  Protocol VLAN Information  Name: "vlan2000"
  EtherType: 0101,0102 LLC: 0201 Snap-EtherType: 0301
  Learning: On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN2000
  IP Address:
  Source MAC address: 00ee.f090.0001(System)
  Description: VLAN2000
  Spanning Tree: MSTP(802.1S)
  IGMP snooping:      MLD snooping:
  Port Information
   0/4           Up   Blocking(STP)   Tagged
   0/6           Up   Blocking(STP)   Untagged
   0/14          Up   Blocking(STP)   Tagged
   0/16          Up   Blocking(STP)   Untagged
   0/19          Up   Forwarding      Untagged
   0/24          Up   Blocking(STP)   Tagged
   0/25          Up   Forwarding      Untagged
   0/26          Up   Blocking(STP)   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 15-14　show vlan summary の実行結果

```
>show vlan summary

Date 2008/03/13 13:13:08 UTC
Total(9)            : 1-3,1999-2001,4092-4094
Port based(3)       : 1,1999,4092
Protocol based(3)   : 2,2000,4094
MAC based(3)        : 3,2001,4093

>
```

（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 15-15 show vlan list の実行結果

```
> show vlan list

Date 2008/03/13 13:13:47 UTC
VLAN counts: 9
  ID Status   Fwd/Up /Cfg Name             Type  Protocol       Ext. IP
   1 Up         3/  7/ 13 VLAN0001         Port  STP MSTP:1S    -    -
   2 Up         2/  8/  8 VLAN0002         Proto STP MSTP:1S    -    -
   3 Up         2/  7/  7 VLAN0003         MAC   STP MSTP:1S    -    -
1999 Up         4/ 14/ 14 VLAN1999         Port  STP MSTP:1S    -    -
2000 Up         2/  8/  8 VLAN2000         Proto STP MSTP:1S    -    -
2001 Up         2/  7/  7 VLAN2001         MAC   STP MSTP:1S    -    -
4092 Up         3/  7/  7 VLAN4092         Port  STP MSTP:1S    -    -
4093 Up         2/  7/  7 VLAN4093         MAC   STP MSTP:1S    -    -
4094 Up         2/  8/  8 VLAN4094         Proto STP MSTP:1S    -    -
     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 15-16 show vlan mac-vlan の実行結果

```
> show vlan mac-vlan

Date 2008/03/13 20:39:25 UTC
VLAN counts: 2    Total MAC Counts: 5
VLAN ID: 2001        MAC Counts: 1
   0001.0123.1230(static)
VLAN ID: 4093        MAC Counts: 4
   0001.0123.1243(static)     0001.0123.1245(static)
   0001.0123.1248(static)     0001.0123.1249(static)

>
```

16 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。

16.1 L2 プロトコルフレーム透過機能の解説

16.1.1 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。

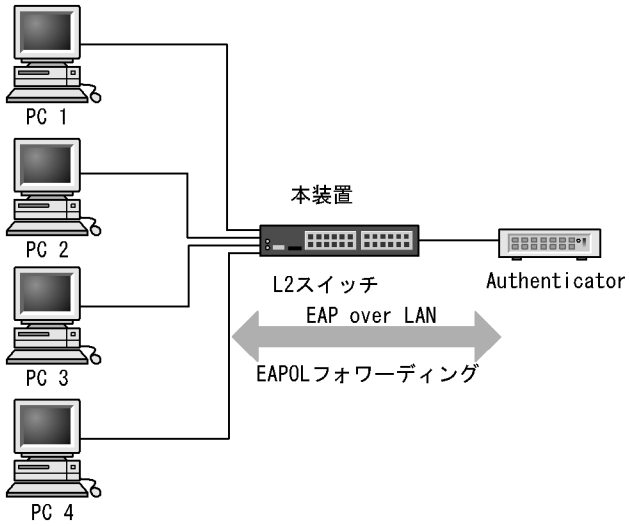
（1） BPDU フォワーディング機能

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 16-1 EAPOL フォワーディング機能の適用例



16.2 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

16.2.1 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 16-1 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。

16.2.2 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。

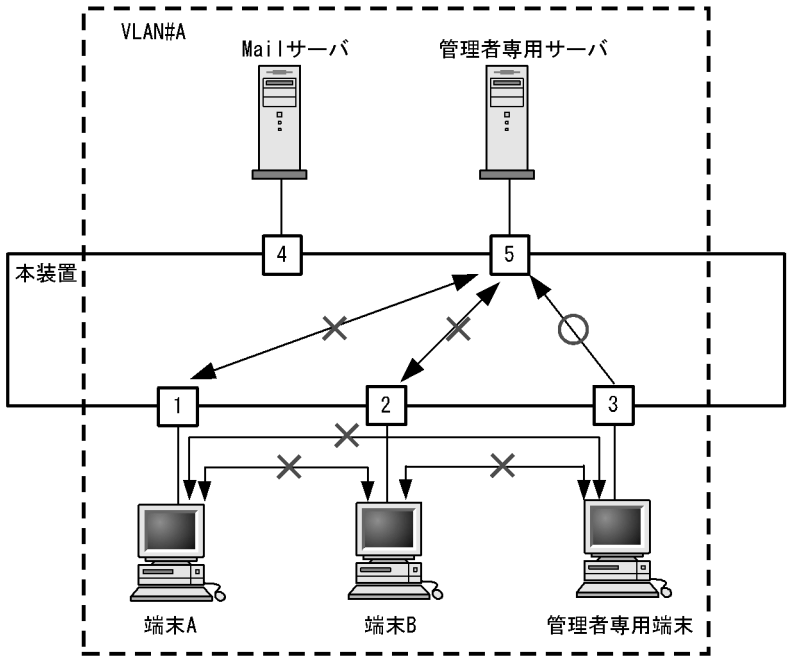
16.3 ポート間中継遮断機能の解説

16.3.1 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 16-2 ポート間中継遮断機能の適用例



・管理者用サーバへは管理者専用端末からだけ通信を許可し，
ほかの端末からの通信を遮断します
・端末間は直接の通信を遮断します
・Mailサーバはすべての端末から通信を可能とします

16.3.2 ポート間中継遮断機能使用時の注意事項

(1) 他機能との共存

ポート間中継遮断機能と下記に示す機能を同時に使用したときの動作を，次の表に示します。

表 16-2 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。

機能	動作
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。
認証専用 IPv4 アクセスリスト（認証前中継）	通信を遮断したポートで認証専用 IPv4 アクセスリストを運用すると，認証前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。

16.4 ポート間中継遮断機能のコンフィグレーション

16.4.1 コンフィグレーションコマンド一覧

ポート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 16-3 コンフィグレーションコマンド一覧

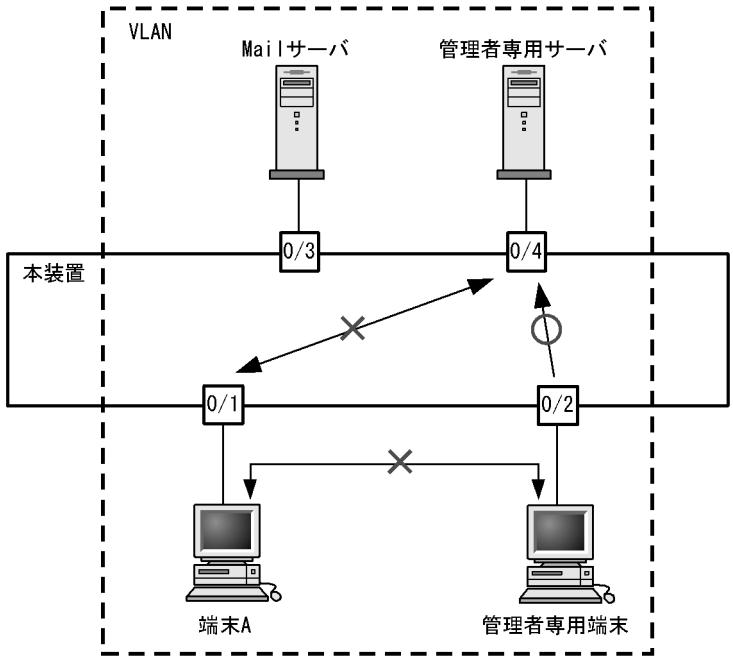
コマンド名	説明
switchport isolation	指定したポートへの中継を遮断します。

16.4.2 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 16-3 ポート間中継遮断機能の設定例



・管理者用サーバへは管理者専用端末からだけ通信を許可し，
ほかの端末からの通信を遮断します
・端末間は直接の通信を遮断します
・Mailサーバはすべての端末から通信を可能とします

[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。

16.4.3 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。

16.5 VLAN 拡張機能のオペレーション

16.5.1 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 16-4 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。

16.5.2 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 16-5 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 16-4 show vlan detail の実行結果

```
> show vlan id 10 detail

Date 2008/03/26 10:12:47 UTC
VLAN counts: 1
VLAN ID: 10    Type: Port based  Status: Up
  Learning:On
  BPDU Forwarding: On     EAPOL Forwarding:                          …1
  Router Interface Name: VLAN0010
  IP Address:
  Source MAC address: 00ee.f006.0001(System)
  Description:VLAN0010
  Spanning Tree: None(-)
  IGMP snooping:      MLD snooping:
  Port Information
   0/5           Up   Forwarding      Tagged
   0/6           Down -               Tagged
   0/7           Up   Forwarding      Tagged

>
```

1. BPDU フォワーディング機能が設定され，EAPOL フォワーディング機能が設定されていないことを示します。

17 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。

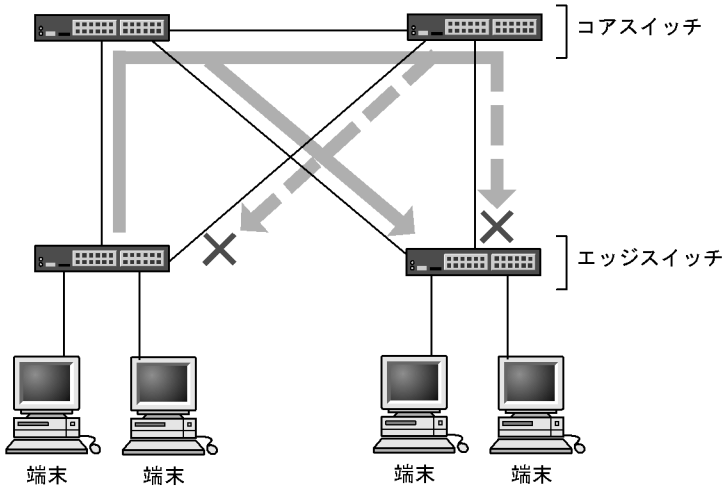
17.1　スパニングツリーの概説

17.1.1　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 17-1　スパニングツリーを適用したネットワークの概要



（凡例）×：Blocking状態

図の構成は，ネットワークのコアを担うスイッチを冗長化し，また，端末を収容するエッジスイッチからの通信経路を冗長化しています。装置および通信経路を冗長化することで，通常の通信経路に障害が発生しても代替の経路で通信を継続できます。

レイヤ 2 ネットワークを冗長化するとレイヤ 2 ループの構成になります。レイヤ 2 のループはブロードキャストストームの発生や MAC アドレス学習が安定しないなどの問題を引き起こします。スパニングツリーは，冗長化してループ構成になったレイヤ 2 ネットワークで，通信を止める場所を選択して Blocking 状態とすることでループを防止するプロトコルです。

17.1.2　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 17-1　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 17-2　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。

17.1.3　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 17-3 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 17-4 Rapid PVST+，Rapid STP(シングルスパニングツリー) の状態遷移

状態	状態の概要	次の状態への遷移
Disable	ポートが使用できない状態です。使用可能となるとすぐに Discarding に遷移します。	－
Discarding	通信不可の状態で，MAC アドレス学習も行いません。該当ポートが Learning になる前に，トポロジーが安定するまで待つ期間です。	省略または 15 秒 (変更可能)
Learning	通信不可の状態です。しかし，MAC 学習は行います。該当ポートが Forwarding になる前に，事前に MAC アドレス学習を行う期間です。	省略または 15 秒 (変更可能)
Forwarding	通信可能の状態です。トポロジーが安定した状態です。	－

（凡例）－：該当なし

Rapid PVST+，Rapid STP では，対向装置からの BPDU 受信によって Discarding と Learning 状態を省略します。この省略により，高速なトポロジー変更を行います。

高速スパニングツリーを使用する際は，以下の条件に従って設定してください。条件を満たさない場合，Discarding，Learning を省略しないで高速な状態遷移を行わない場合があります。

- トポロジーの全体を同じプロトコル（Rapid PVST+ または Rapid STP）で構築する（Rapid PVST+ と Rapid STP の相互接続は「17.3.2 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。

17.1.4 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 17-5 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 17-6 ポートの役割

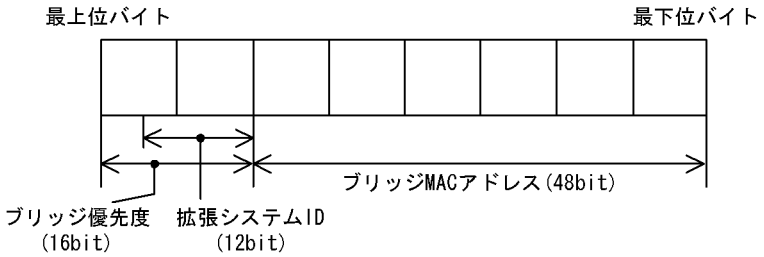
ポートの役割	概要
ルートポート	指定ブリッジからルートブリッジへ向かう通信経路のポートです。通信可能なポートとなります。
指定ポート	ルートポート以外の通信可能なポートです。ルートブリッジからの通信経路でトポロジーの下流へ接続するポートです。
非指定ポート	ルートポート，指定ポート以外のポートで，通信不可の状態のポートです。障害が発生した際に通信可能になり代替経路として使用します。

(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 17-2 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

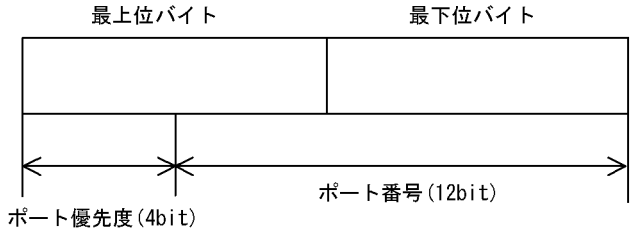
トの速度に応じた値となっていて，コンフィグレーションで変更することもできます。

(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。

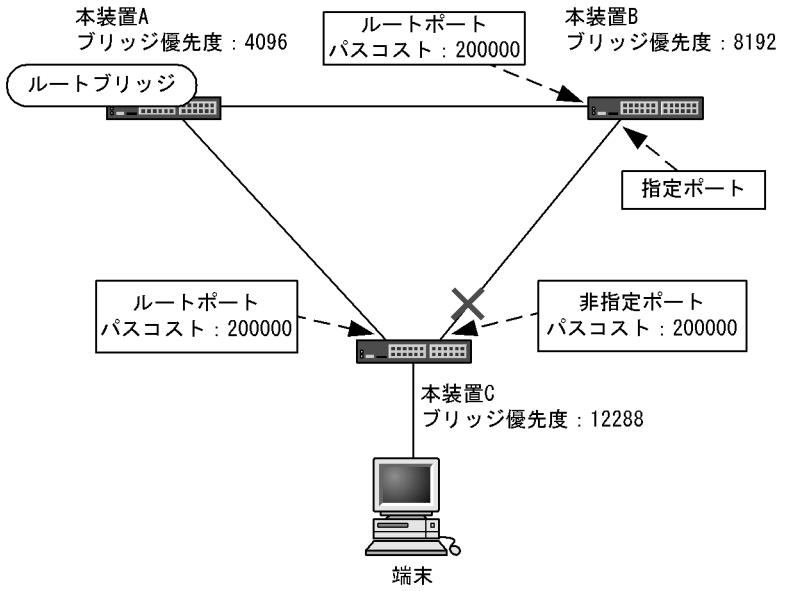
図 17-3 ポート識別子



17.1.5 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 17-4 スパニングツリーのトポロジー設計



（凡例） × ：Blocking状態

(1) ブリッジ識別子によるルートブリッジの選出

ルートブリッジは，ブリッジ識別子の最も小さい装置を選出します。通常，ルートブリッジにしたい装置のブリッジ優先度を最も小さい値（最高優先度）に設定します。図の例では，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。

17.1.6 STP 互換モード

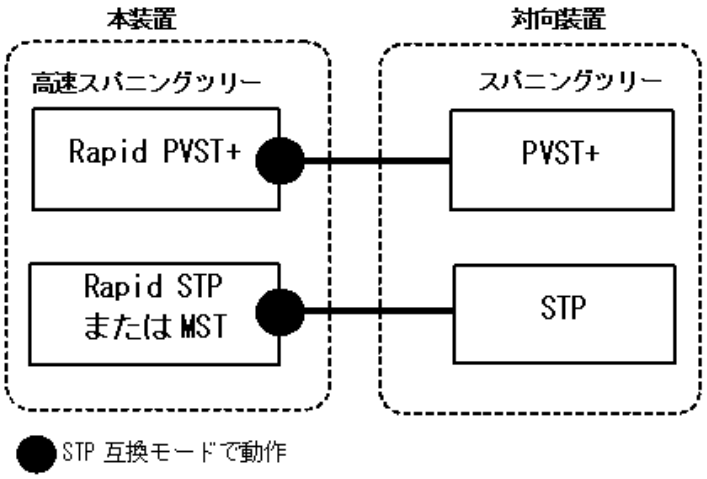
(1) 概要

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 17-5 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，「17.1.4 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 17-6 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。

17.1.7　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。

17.2 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。

17.2.1 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 17-7 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。

17.2.2 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 17-8 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。

17.3　PVST+ 解説

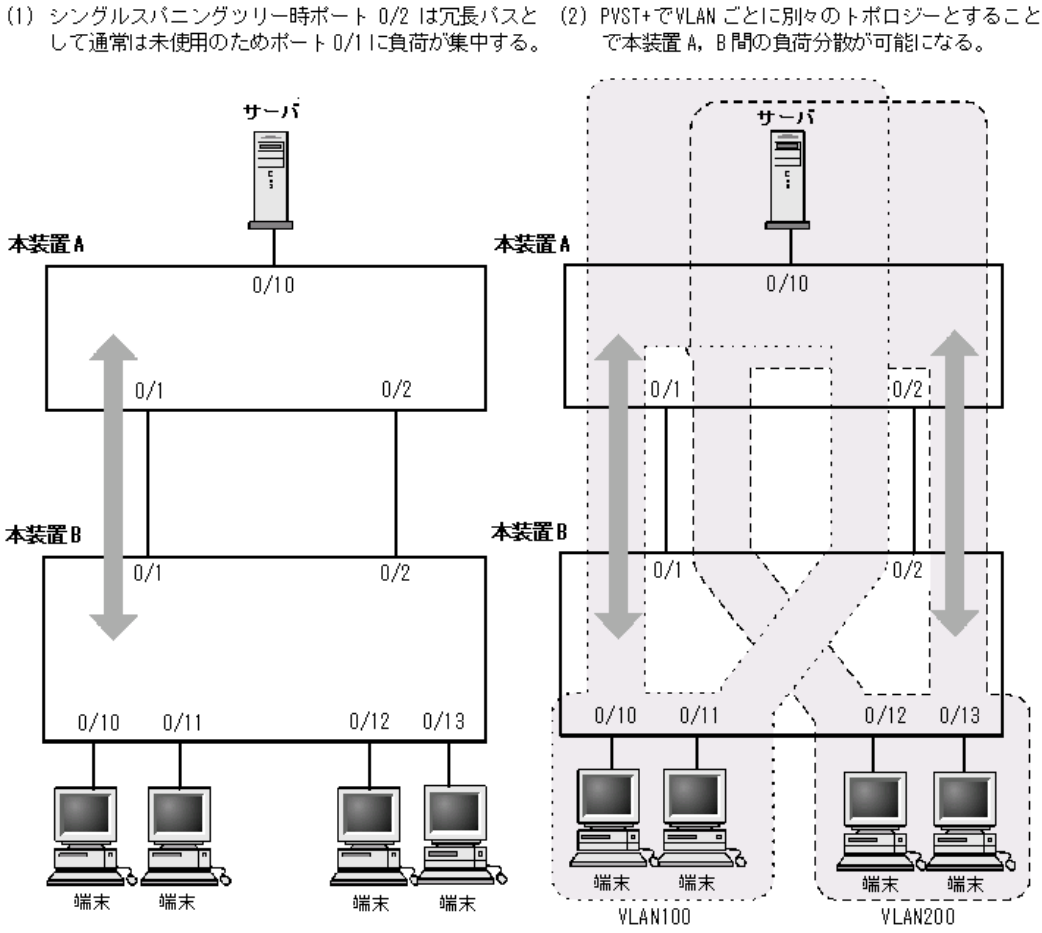
PVST+ は，VLAN 単位にツリーを構築します。VLAN 単位にツリーを構築できるため，ロードバランシングが可能です。また，アクセスポートでは，シングルスパニングツリーで動作しているスイッチと接続できます。

17.3.1　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 17-6　PVST+ によるロードバランシング



17.3.2 アクセスポートの PVST+

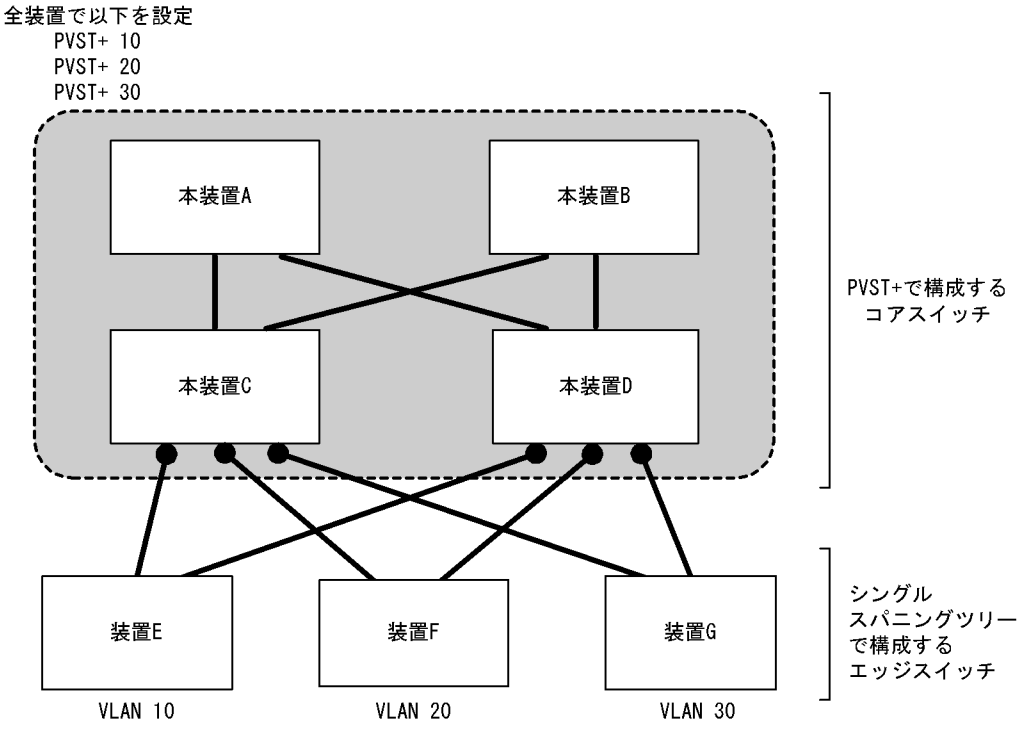
(1) 解説

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 17-7 シングルスパニングツリーとの接続



（凡例） ●：アクセスポート

(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。

17.3.3　PVST+ 使用時の注意事項

（1） 他機能との共存

「13.3　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

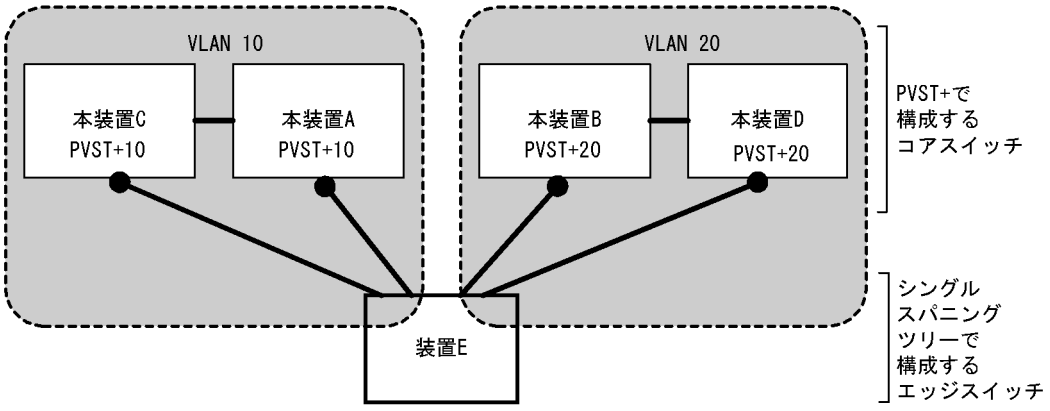
シングルスパニングツリーと VLAN 1 の PVST+ を同時に動作させることはできません。シングルスパニングツリーを動作させると VLAN 1 の PVST+ は停止します。

（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 17-8　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。

17.4 PVST+ のコンフィグレーション

17.4.1 コンフィグレーションコマンド一覧

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 17-9 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。

17.4.2 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。

17.4.3　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 17-10　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。

17.4.4 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。

17.5　PVST+ のオペレーション

17.5.1　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 17-11　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。

17.5.2　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 17-9　show spanning-tree の実行結果

```
> show spanning-tree vlan 2001

Date 2006/12/13 15:58:20 UTC
VLAN 2001  PVST+ Spanning Tree:Enabled   Mode:PVST+
  Bridge ID       Priority: 34769     MAC Address: 00ee.f211.0001
    Bridge Status: Designated
  Root Bridge ID  Priority: 34769     MAC Address: 0012.e238.0d33
    Root Cost: 6
    Root Port: 0/17-24(ChGr: 2)
  Port Information
    0/1       Up   Status:Forwarding  Role:Designated   PortFast
    0/11      Up   Status:Blocking    Role:Alternate    -
    0/12      Up   Status:Blocking    Role:Alternate    -
    0/13      Up   Status:Blocking    Role:Alternate    -
    0/14      Up   Status:Blocking    Role:Alternate    -
    0/15      Up   Status:Blocking    Role:Alternate    -
    0/16      Up   Status:Blocking    Role:Alternate    -
    0/25      Up   Status:Blocking    Role:Alternate    -
    0/26      Up   Status:Blocking    Role:Alternate    -
    ChGr:2    Up   Status:Forwarding  Role:Root         -

>
```

17.6 シングルスパニングツリー解説

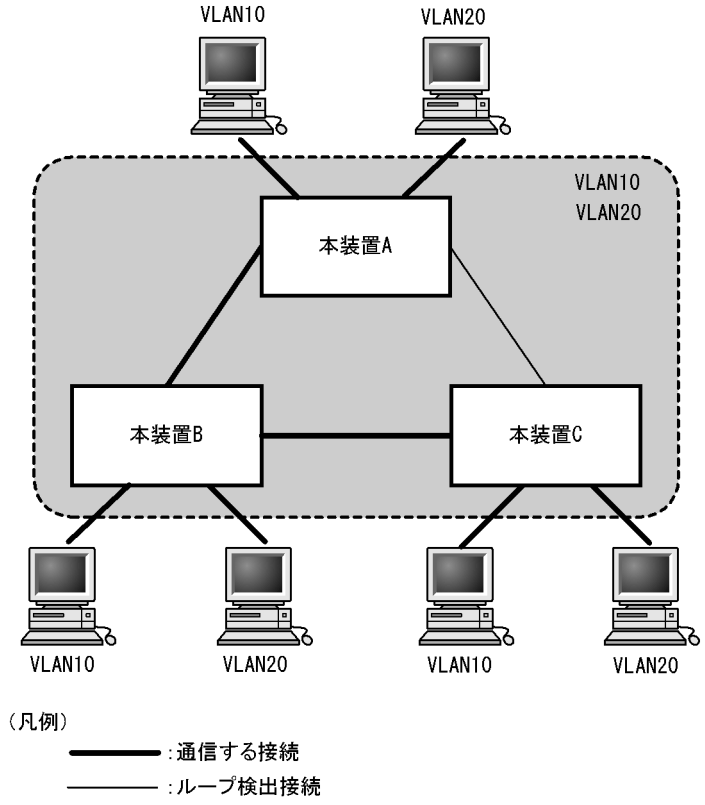
シングルスパニングツリーは装置全体を対象としトポロジーを構築します。

17.6.1 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 17-10 シングルスパニングツリーによるネットワーク構成



17.6.2 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 17-12　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。

17.6.3　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

「13.3　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。

17.7 シングルスパニングツリーのコンフィグレーション

17.7.1 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 17-13 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。

17.7.2 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。

17.7.3 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 17-14 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。

17.7.4 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。

17.8　シングルスパニングツリーのオペレーション

17.8.1　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 17-15　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。

17.8.2　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 17-11　シングルスパニングツリーの情報

```
> show spanning-tree single

Date 2006/12/13 15:28:32 UTC
Single Spanning Tree:Enabled   Mode:STP
  Bridge ID       Priority: 32768     MAC Address: 00ee.f209.0001
    Bridge Status: Designated
  Root Bridge ID  Priority: 32768     MAC Address: 0012.e208.16a6
    Root Cost: 2
    Root Port: 0/9-16(ChGr: 2)
  Port Information
    0/1       Up   Status:Forwarding  Role:Designated   PortFast
    0/2       Up   Status:Forwarding  Role:Designated   PortFast
    ChGr:1    Down Status:Disabled    Role:-            PortFast
    ChGr:2    Up   Status:Forwarding  Role:Root         PortFast
    ChGr:3    Down Status:Disabled    Role:-            PortFast
    ChGr:4    Down Status:Disabled    Role:-            PortFast

>
```

17.9　マルチプルスパニングツリー解説

17.9.1　概要

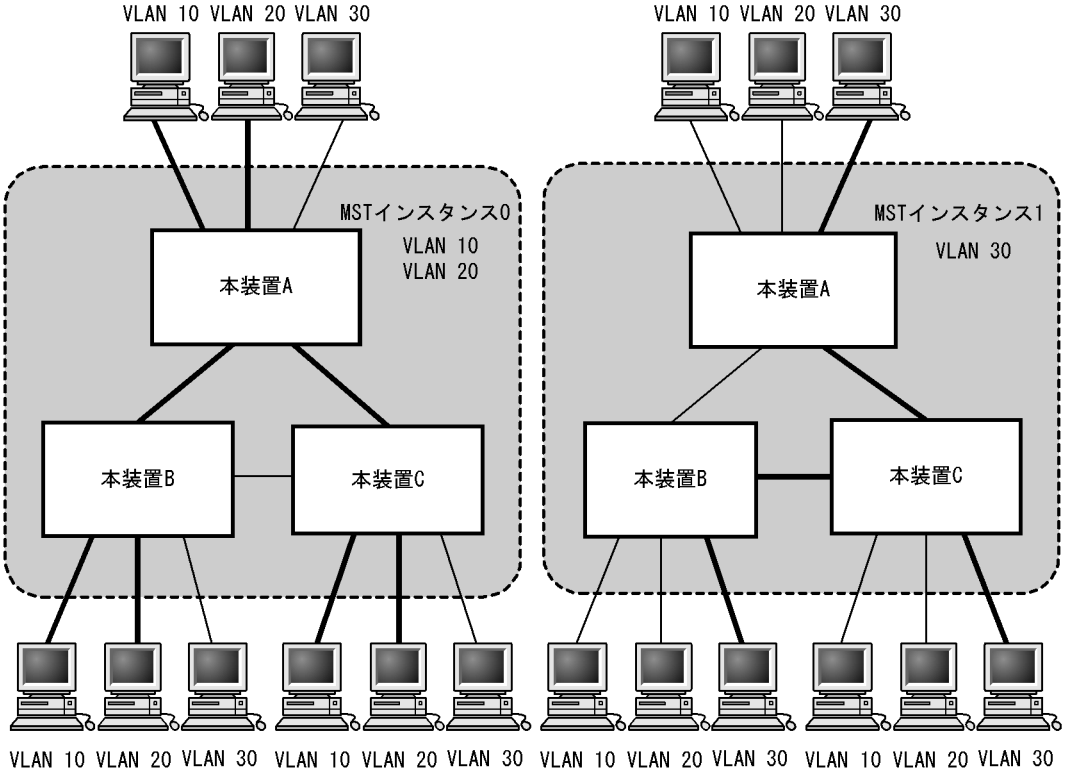
マルチプルスパニングツリーには，次の特長があります。MST インスタンスによってロードバランシングを可能にしています。また，MST リージョンによって，大規模なネットワーク構成を中小構成に分割することでネットワーク設計が容易になります。以降，これらを実現するためのマルチプルスパニングツリーの機能概要を説明します。

（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 17-12　MST インスタンスイメージ



ネットワーク上に，二つのインスタンスを定義して，ロードバランシングしています。
インスタンス0には，VLAN 10，20を所属させ，インスタンス1には，VLAN 30を所属させています。

（凡例）
：通信する接続
：ループ検出接続，
　および通信しない接続

（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

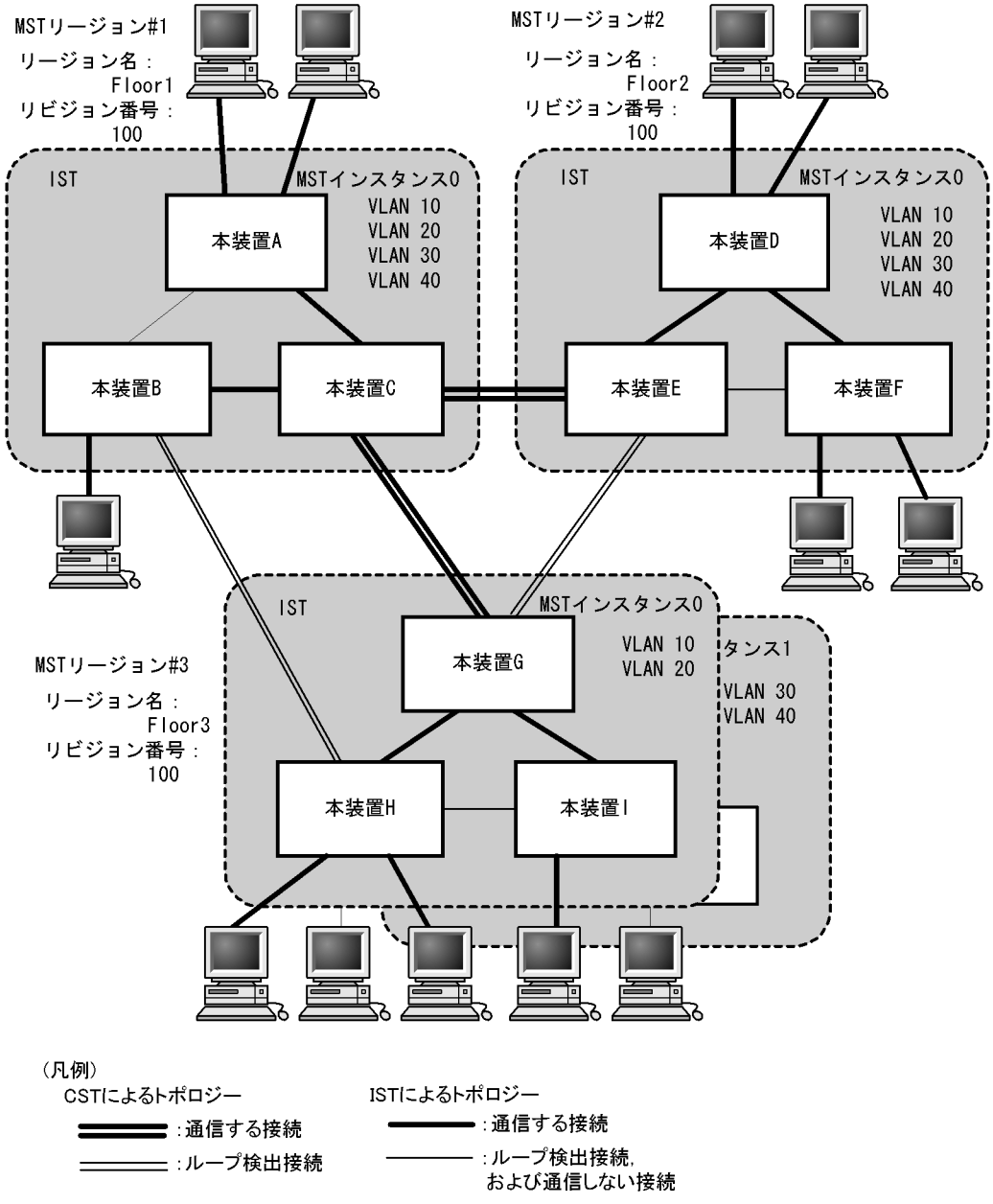
BPDU を送受信する唯一の MST インスタンスとなります。全 MST インスタンスのトポロジー情報は，MST BPDU にカプセル化し通知します。

● 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 17-13　マルチプルスパニングツリー概要



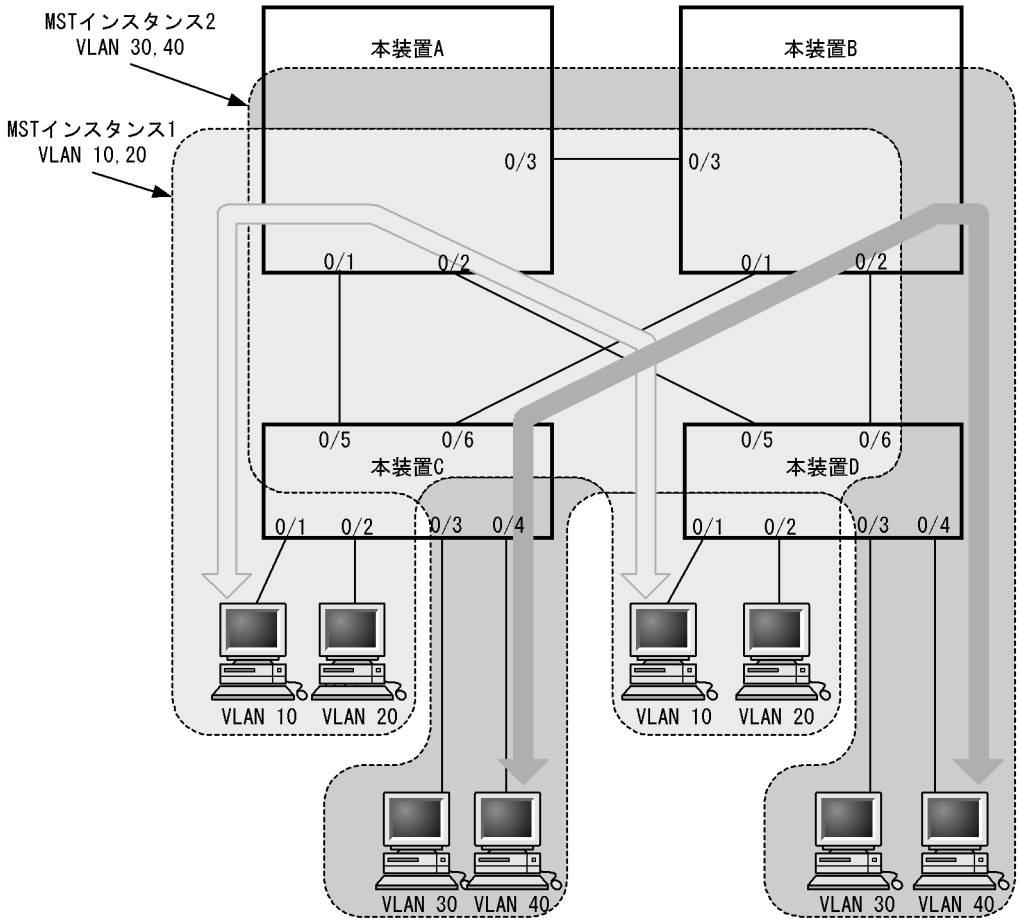
17.9.2　マルチプルスパニングツリーのネットワーク設計

（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 17-14　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



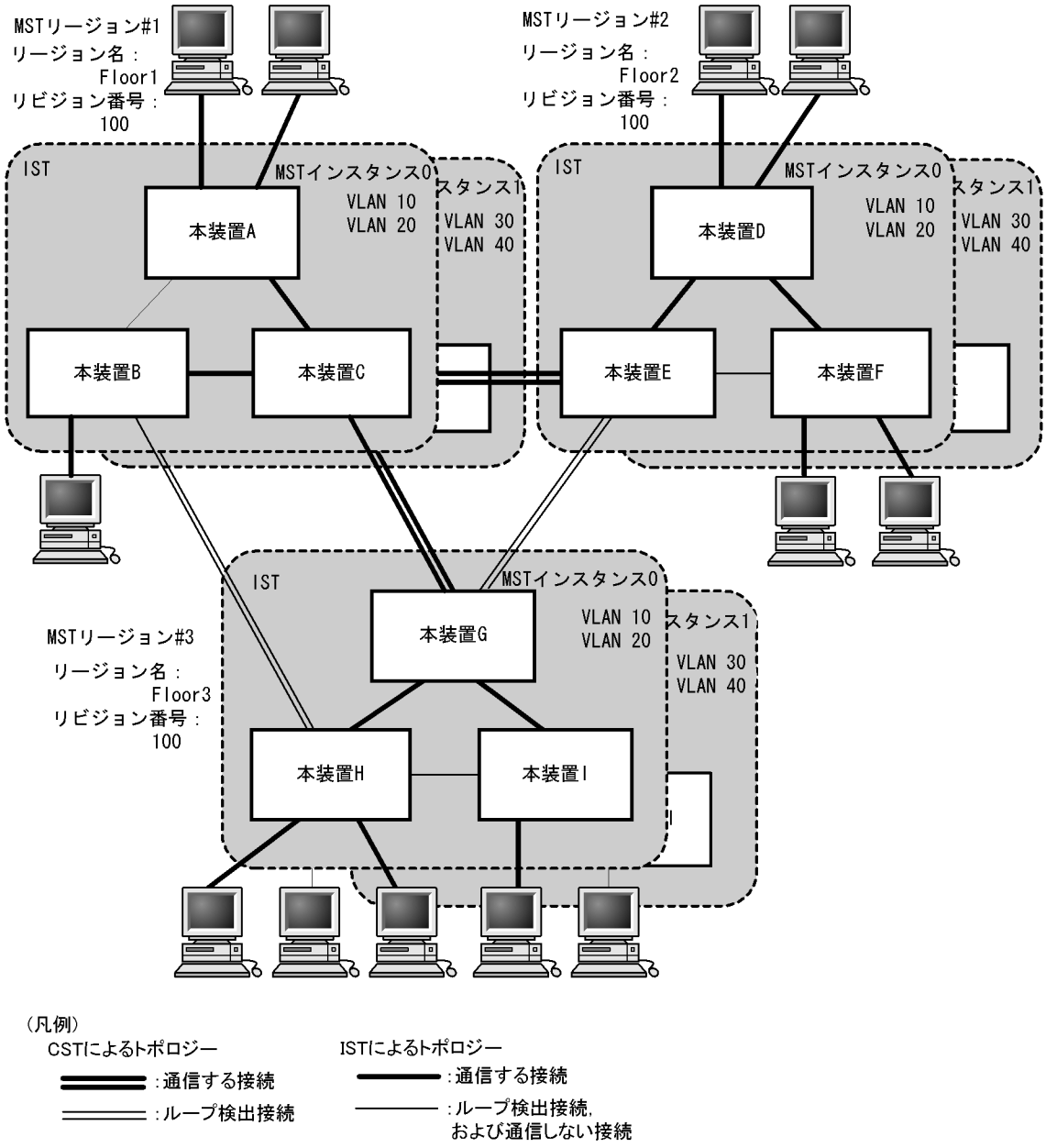
本装置Cと本装置Dに接続しているVLAN10の端末の通信経路と，本装置Cと本装置Dに接続しているVLAN40の端末で通信経路をロードバランシングしています。

（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 17-15　MST リージョンによるネットワーク構成



17.9.3　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。

17.9.4　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

「13.3　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 17-16　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

17.10 マルチプルスパニングツリーのコンフィグレーション

17.10.1 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 17-17 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。

17.10.2 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。

17.10.3 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 17-18 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。

17.10.4 マルチプルスパニングツリーのパラメータ設定

各パラメータは「2 × (forward-time − 1) ≧ max-age ≧ 2 × (hello-time + 1)」という関係が成立するように設定する必要があります。パラメータを変える場合はトポロジー全体でパラメータを合わせる必要があります。

(1) BPDU の送信間隔の設定

BPDU の送信間隔は，短くした場合はトポロジー変更を検知しやすくなります。長くした場合はトポロジー変更の検知までに時間が掛かるようになる一方で，BPDU トラフィックや本装置のスパニングツリーの負荷を軽減できます。

[設定のポイント]

設定しない場合，2 秒間隔で BPDU を送信します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree mst hello-time 3**
   マルチプルスパニングツリーの BPDU 送信間隔を 3 秒に設定します。

[注意事項]

BPDU の送信間隔を短くすると，トポロジー変更を検知しやすくなる一方で BPDU トラフィックが増加することによりスパニングツリーの負荷が増加します。本パラメータをデフォルト値（2 秒）より短くすることによってタイムアウトのメッセージ出力やトポロジー変更が頻発する場合は，デフォルト値に戻して使用してください。

(2) 送信する最大 BPDU 数の設定

スパニングツリーでは，CPU 負荷の増大を抑えるために，hello-time（BPDU 送信間隔）当たりに送信す

る最大 BPDU 数を決めることができます。トポロジー変更が連続的に発生すると，トポロジー変更を通知，収束するために大量の BPDU が送信され，BPDU トラフィックの増加，CPU 負荷の増大につながります。送信する BPDU の最大数を制限することによりこれらを抑えます。

[設定のポイント]

設定しない場合，hello-time（BPDU 送信間隔）当たりの最大 BPDU 数は 3 で動作します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree mst transmission-limit 5**
   マルチプルスパニングツリーの hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

(3) 最大ホップ数の設定

ルートブリッジから送信する BPDU の最大ホップ数を設定します。BPDU のカウンタは装置を経由するたびに増加し，最大ホップ数を超えた BPDU は無効な BPDU となって無視されます。

シングルスパニングツリーの装置と接続しているポートは，最大ホップ数（max-hops）ではなく最大有効時間（max-age）のパラメータを使用します。ホップ数のカウントはマルチプルスパニングツリーの装置間で有効なパラメータです。

[設定のポイント]

最大ホップ数を大きく設定することによって，多くの装置に BPDU が届くようになります。設定しない場合，最大ホップ数は 20 で動作します。

[コマンドによる設定]

1. **(config)# spanning-tree mst max-hops 10**
   マルチプルスパニングツリーの BPDU の最大ホップ数を 10 に設定します。

(4) BPDU の最大有効時間の設定

マルチプルスパニングツリーでは，最大有効時間（max-age）はシングルスパニングツリーの装置と接続しているポートでだけ有効なパラメータです。トポロジー全体をマルチプルスパニングツリーが動作している装置で構成する場合は設定する必要はありません。

最大有効時間は，ルートブリッジから送信する BPDU の最大有効時間を設定します。BPDU のカウンタは装置を経由するたびに増加して，最大有効時間を超えた BPDU は無効な BPDU となって無視されます。

[設定のポイント]

最大有効時間を大きく設定することで，多くの装置に BPDU が届くようになります。設定しない場合，最大有効時間は 20 で動作します。

[コマンドによる設定]

1. **(config)# spanning-tree mst max-age 25**
   マルチプルスパニングツリーの BPDU の最大有効時間を 25 秒に設定します。

(5) 状態遷移時間の設定

タイマによる動作となる場合，ポートの状態が Discarding から Learning，Forwarding へ一定時間ごと

に遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると，より早く Forwarding 状態に遷移できます。

［設定のポイント］

設定しない場合，状態遷移時間は 15 秒で動作します。本パラメータを短い時間に変更する場合，BPDU の最大有効時間（max-age），送信間隔（hello-time）との関係が「2 × (forward-time − 1) ≧ max-age ≧ 2 × (hello-time + 1)」を満たすように設定してください。

［コマンドによる設定］

1. **(config)# spanning-tree mst forward-time 10**
   マルチプルスパニングツリーの BPDU の状態遷移時間を 10 秒に設定します。

17.11　マルチプルスパニングツリーのオペレーション

17.11.1　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 17-19　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。

17.11.2　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 17-16 show spanning-tree の実行結果

```
> show spanning-tree mst

Date 2006/12/15 13:32:33 UTC
Multiple Spanning Tree: Enabled
Revision Level: 65535  Configuration Name: Kanagawa
CIST Information
  VLAN Mapped: 1,3-4093,4095                                    ••••1
  CIST Root      Priority: 4096        MAC      : 00ee.f207.0001
  External Root Cost     : 0           Root Port: 0/25-26(ChGr: 1)
  Regional Root  Priority: 4096        MAC      : 00ee.f207.0001
  Internal Root Cost     : 2000
  Bridge ID      Priority: 32768       MAC      : 00ee.f212.0001
  Regional Bridge Status : Designated
  Port Information
    0/5       Up   Status:Forwarding  Role:Designated   Boundary Compatible
    0/7       Up   Status:Forwarding  Role:Designated   -
    0/11      Up   Status:Forwarding  Role:Designated   BPDUGuard
    ChGr:1    Up   Status:Forwarding  Role:Root         -
    ChGr:2    Up   Status:Discarding  Role:Alternate    -
MST Instance 1
  VLAN Mapped: 2,4094
  Regional Root  Priority: 32769       MAC      : 00ee.f207.0001
  Internal Root Cost     : 2000        Root Port: 0/1-4(ChGr: 2)
  Bridge ID      Priority: 32769       MAC      : 00ee.f212.0001
  Regional Bridge Status : Designated
  Port Information
    0/5       Up   Status:Forwarding  Role:Designated   Boundary Compatible
    0/7       Up   Status:Forwarding  Role:Designated   -
    ChGr:2    Up   Status:Forwarding  Role:Root         -

>
```

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。

17.12 スパニングツリー共通機能解説

17.12.1 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 17-20 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。

（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。

17.12.2　BPDU フィルタ

（1） 概要

BPDU フィルタ機能を適用したポートでは，BPDU の送受信を停止します。

（2） BPDU フィルタに関する注意事項

PortFast を適用したポート以外に BPDU フィルタ機能を設定した場合，トポロジーにループが発生するおそれがあるため，注意してください。

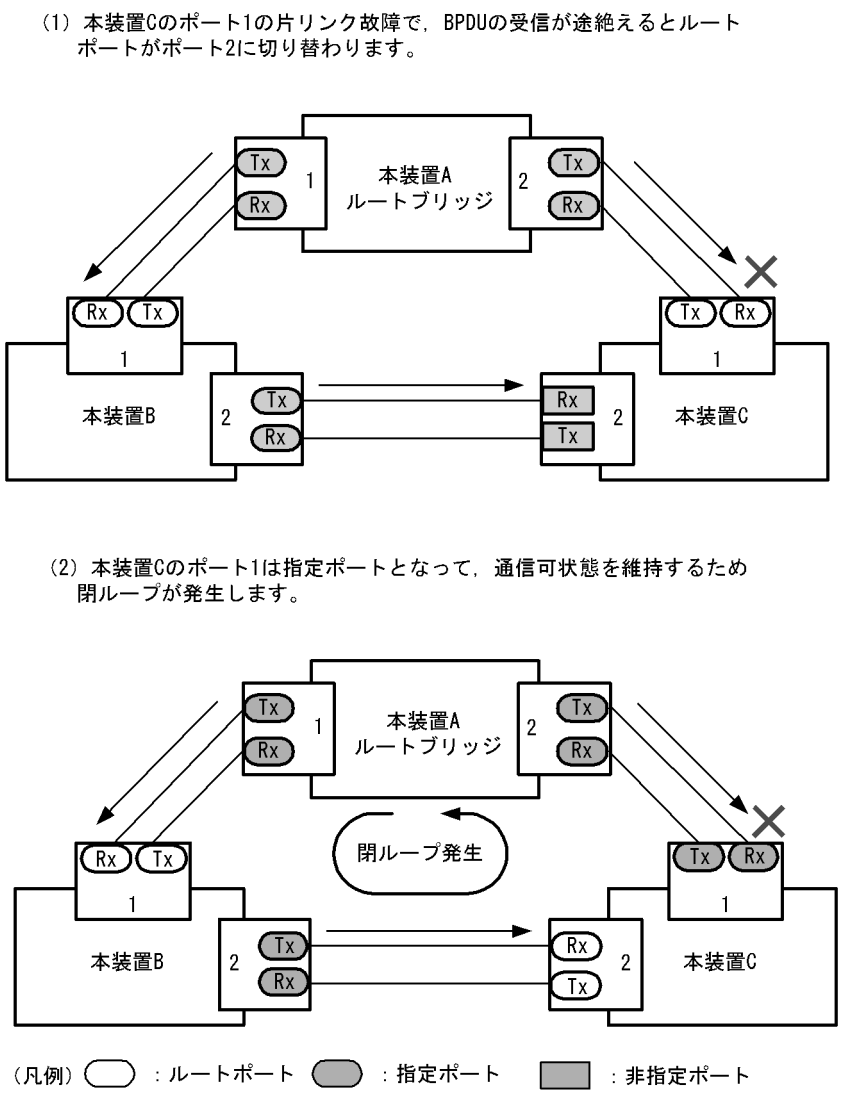
17.12.3 ループガード

(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 17-17 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 17-21　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。

17.12.4　ルートガード

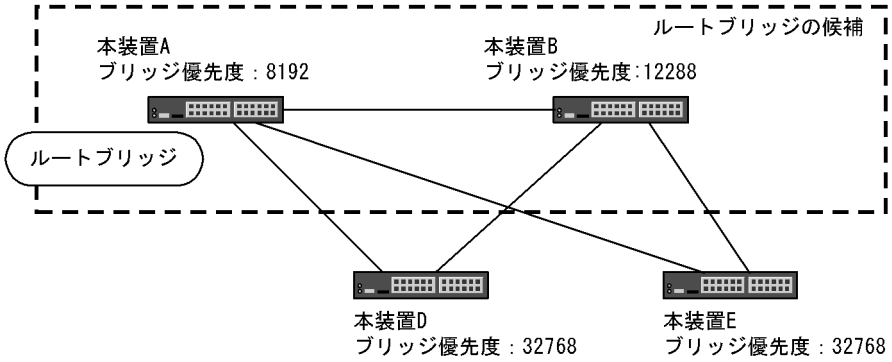
（1） 概要

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。

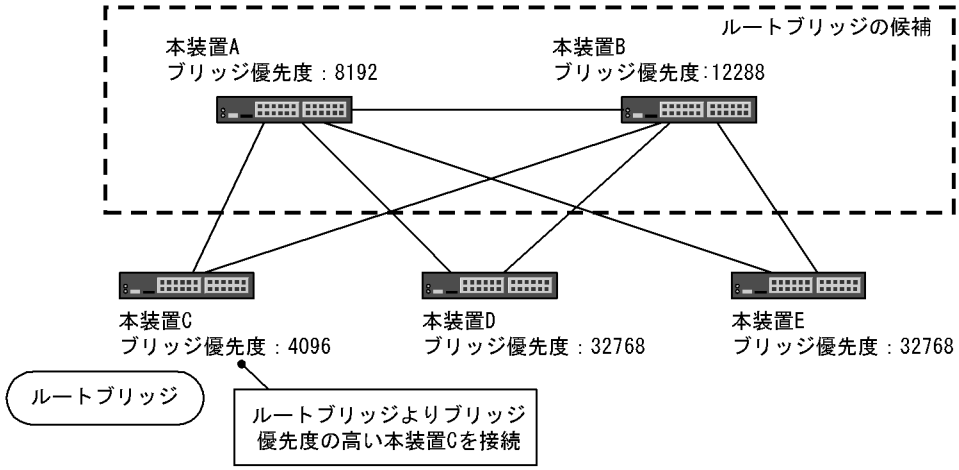
● 本装置 A，本装置 B をルートブリッジの候補として運用

図 17-18　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 17-19 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 17-22 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

17.13　スパニングツリー共通機能のコンフィグレーション

17.13.1　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 17-23　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。

17.13.2　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。

17.13.3 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。

17.13.4 ループガードの設定

片線切れなどの単一方向のリンク障害が発生し，BPDU の受信が途絶えた場合，ループが発生することがあります。ループガードは，このようなループの発生を防止したい場合に設定します。

［設定のポイント］

ループガードは，PortFast 機能を設定していないポートで動作します。

spanning-tree loopguard default コマンドを設定すると，PortFast を設定したポート以外のすべてのポートにループガードを適用します。デフォルトで適用する場合に，ループガードを無効にしたい場合は spanning-tree guard none コマンドを設定します。

［コマンドによる設定］

1. **(config)# spanning-tree loopguard default**
   PortFast を設定したポート以外のすべてのポートに対してループガード機能を適用するように設定します。

2. **(config)# interface 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。

17.13.5 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。

17.13.6 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。

17.14　スパニングツリー共通機能のオペレーション

17.14.1　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 17-24　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。

17.14.2　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 10 の PVST+ の例を次の図に示します。

PortFast はポート 0/3，0/4，0/5 に設定していることを PortFast の項目で確認できます。ポート 0/3 は PortFast を設定していて，ポート 0/4 は PortFast に加えて BPDU ガードを設定しています。どちらのポートも意図しない BPDU を受信しないで正常に動作していることを示しています。ポート 0/5 は BPDU フィルタを設定しています。

リンクタイプは各ポートの Link Type の項目で確認できます。すべてのポートが point-to-point で動作しています。

図 17-20　スパニングツリーの情報

```
> show spanning-tree vlan 2001 detail

Date 2006/12/13 16:06:34 UTC
VLAN 10  PVST+ Spanning Tree:Enabled   Mode:Rapid PVST+
  Bridge ID
    Priority:32778                 MAC Address:00ee.f005.0001
    Bridge Status:Root             Path Cost Method:Short
    Max Age:20                     Hello Time:2
    Forward Delay:15
  Root Bridge ID
    Priority:32778                 MAC Address:00ee.f005.0001
    Root Cost:0
    Root Port:-
    Max Age:20                     Hello Time:2
    Forward Delay:15
  Port Information
  Port:0/3 Up
    Status:Forwarding              Role:Designated
    Priority:128                   Cost:19
    Link Type:point-to-point       Compatible Mode:-
    Loop Guard:OFF                 PortFast:ON(BPDU not received)
    BPDUFilter:OFF                 RootGuard:OFF
  Port:0/4 Up
    Status:Forwarding              Role:Designated
    Priority:128                   Cost:19
    Link Type:point-to-point       Compatible Mode:-
    Loop Guard:OFF                 PortFast:BPDU Guard(BPDU not received)
    BPDUFilter:OFF                 RootGuard:OFF
  Port:0/5 Up
    Status:Forwarding              Role:Designated
    Priority:128                   Cost:19
    Link Type:point-to-point       Compatible Mode:-
    Loop Guard:OFF                 PortFast:ON(BPDU not received)
    BPDUFilter:ON                  RootGuard:OFF

>
```

18 DHCP snooping

この章では，DHCP snooping の解説と操作方法について説明します。

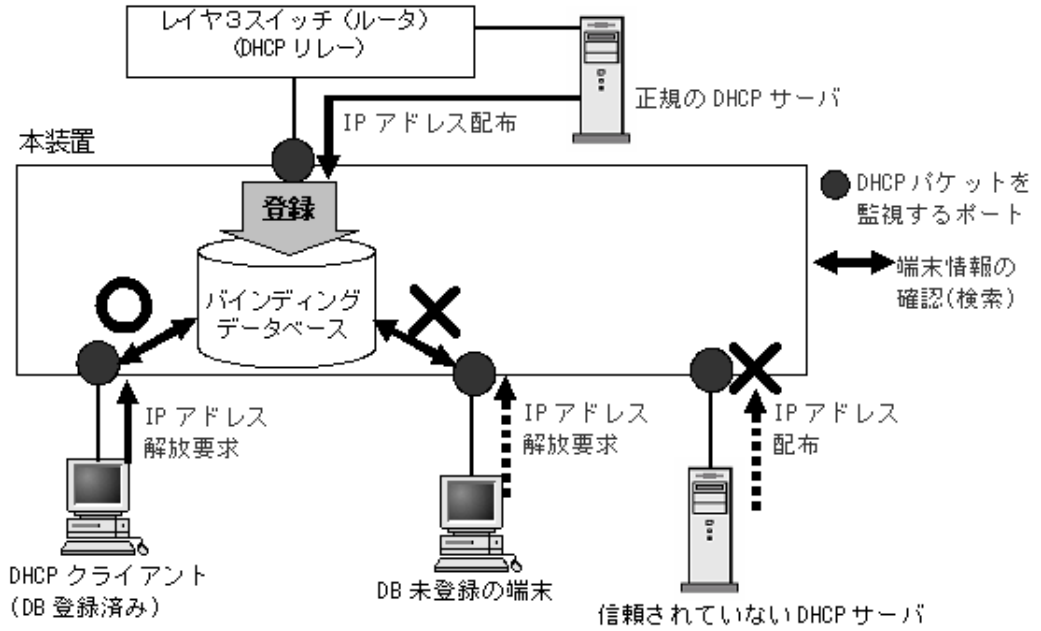
18.1 DHCP snooping 機能の解説

DHCP snooping は，本装置を通過する DHCP パケットを監視して，信頼されていない端末からのアクセスを制限する機能です。

- DHCP サーバから IP アドレスを配布されたクライアントと固定 IP アドレス端末を，バインディングデータベースに登録して管理します。
- 信頼されていない端末（バインディングデータベース未登録の端末のこと。以下，DB 未登録の端末と表記）からの，IP アドレス解放要求を抑止します。
- 信頼されていない DHCP サーバからの IP アドレス配布を抑止します。

DHCP snooping は，次の図に示すように DHCP サーバと DHCP クライアントの間に本装置を接続して使用します。

図 18-1 DHCP snooping 概要



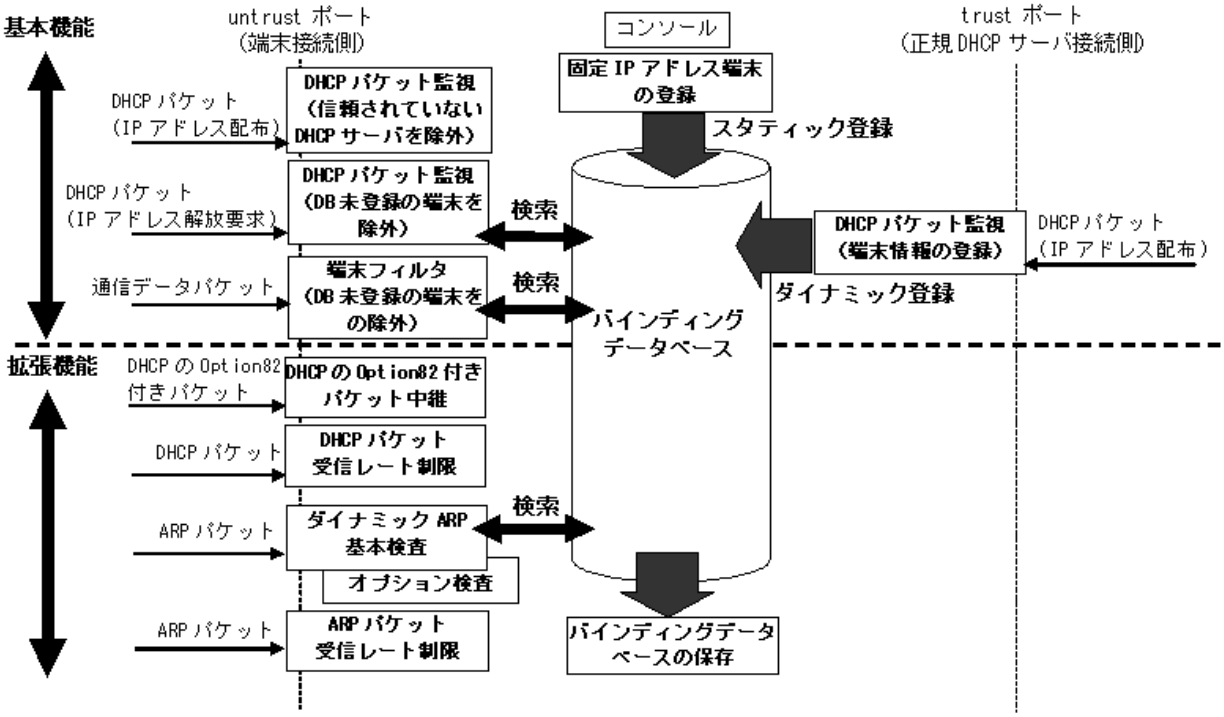
また，DB 未登録の端末からの通信データパケットをすべて廃棄する，端末フィルタ機能をサポートしています。

DHCP snooping は，上記のほかに拡張機能として下記をサポートしています。

- DHCP の Option82 付きパケットの中継
- DHCP パケットの受信レート制限
- ダイナミック ARP 検査機能
- バインディングデータベースの保存

各機能とバインディングデータベースの動作関係を次の図に示します。

図 18-2　各機能とバインディングデータベースの動作関係図



各機能の詳細説明や設定説明は下記を参照してください。

表 18-1　DHCP snooping のサポート機能

機能	項目	機能説明参照先	設定説明参照先
基本	DHCP パケットの監視	「18.1.1」参照	「18.2.4」参照
	端末フィルタ	「18.1.2」参照	「18.2.4」参照
	固定 IP アドレス端末の通信許可	「18.1.2」参照	「18.2.4」参照
拡張	DHCP の Option82 付きパケットの中継	「18.1.3」参照	「18.2.5」参照
	DHCP パケットの受信レート制限	「18.1.4」参照	「18.2.6」参照
	ダイナミック ARP 検査機能		
	基本検査	「18.1.5」参照	「18.2.7」参照
	オプション検査	「18.1.5」参照	「18.2.7」参照
	ARP パケットの受信レート制限	「18.1.5」参照	「18.2.7」参照
	バインディングデータベースの保存		
	書き込み指定時間満了時の保存	「18.1.6」参照	「18.2.8」参照
	特定オペレーションによる保存	「18.1.6」参照	－

18.1.1　DHCP パケットの監視

(1) ポートの種別と DHCP パケット監視動作

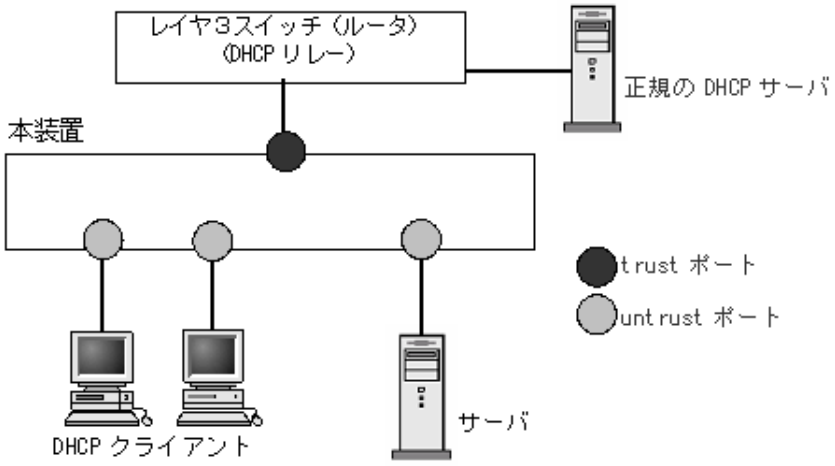
DHCP snooping では，ポートを下記の種別に分類して，DHCP パケットを監視します。

1. trust ポート

正規の DHCP サーバを接続するポートです。
trust ポートで受信した DHCP サーバからのパケットを監視し，バインディングデータベースに端末情報をダイナミック登録します。

2. untrust ポート
DHCP クライアントや部門サーバなど，不特定の端末を接続するポートであり，DHCP サーバは接続しません。

図 18-3 DHCP snooping のポート種別

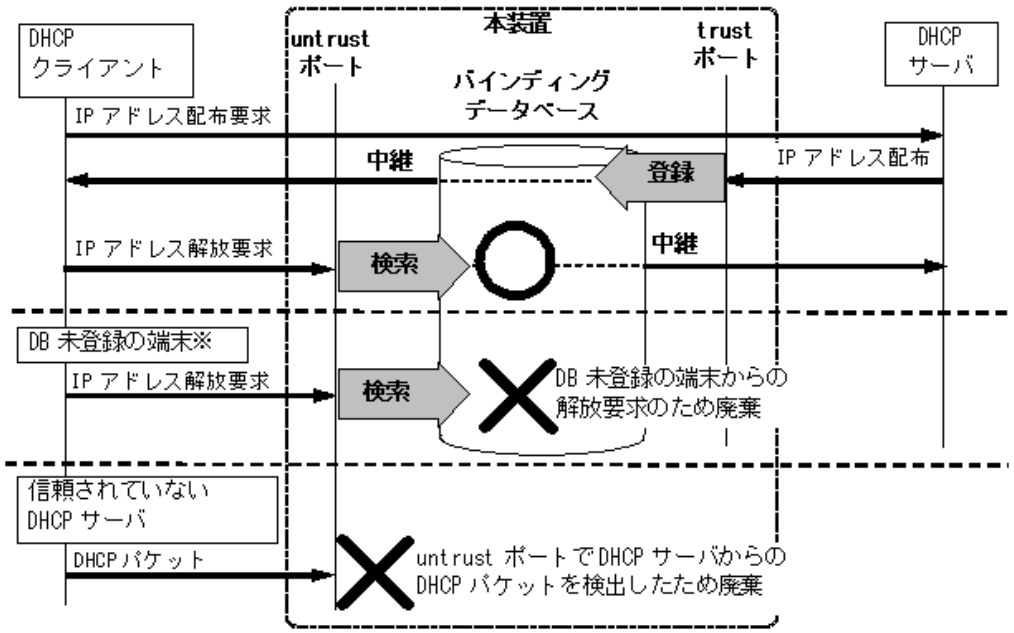


untrust ポートに接続された端末を対象に DHCP パケットを監視し，下記のアクセスを除外します。

- DB 未登録の端末からの IP アドレス解放要求を抑止
untrust ポートで，DB 未登録の端末から IP アドレス解放要求を受信したときは廃棄します。これにより，正規の DHCP サーバから IP アドレスを配布された形跡のない端末からの IP アドレス解放要求を抑止することができます。
- DHCP サーバからの DHCP パケットを廃棄
untrust ポートで，受信した DHCP パケットを監視し，DHCP サーバからのパケットを検出したときは廃棄します。これにより，信頼されていない DHCP サーバからの IP アドレス配布を抑止することができます。

DHCP パケット監視の動作概要を次の図に示します。

図 18-4 DHCP パケット監視の動作概要



注※DB 未登録の端末：バインディングデータベースに未登録の端末

コンフィグレーションコマンド ip dhcp snooping で DHCP snooping を有効にすると，デフォルトで全ポートが untrust ポートになります。正規の DHCP サーバへ接続するポートを trust ポートとして設定してください。trust ポートはコンフィグレーションコマンド ip dhcp snooping trust で設定できます。

(2) バインディングデータベースの登録

バインディングデータベースの登録には，ダイナミック登録とスタティック登録があります。

- ダイナミック登録：DHCP サーバから IP アドレスが配布されたときに登録
- スタティック登録：コンフィグレーションコマンド ip source binding で登録

バインディングデータベースの登録内容は，下記のとおりです。

表 18-2 バインディングデータベースの登録内容

項目		ダイナミック登録	スタティック登録
エントリ数	246 エントリ	ダイナミック・スタティックの合計登録値です。 （うち，スタティック登録は最大 64 エントリまで登録可能）	
登録内容	端末の MAC アドレス	DHCP クライアントの MAC アドレス	固定 IP アドレス端末の MAC アドレス
	端末の IP アドレス	DHCP サーバから配布された IP アドレス	固定 IP アドレス端末の IP アドレス
		ダイナミック・スタティックともに，下記の範囲が有効 • 1.0.0.0 ～ 126.255.255.255 • 128.0.0.0 ～ 223.255.255.255	
	端末の VLAN ID	端末を接続するポートまたはチャネルグループの所属する VLAN ID	

項目		ダイナミック登録	スタティック登録
	端末のポート番号	端末を接続するポート番号またはチャネルグループ番号	
エージングタイマ	リース時間	ダイナミック登録してからエントリをエージングするまでの時間です。DHCP サーバから配布された IP アドレスのリース時間を適用します。	エージング対象外

18.1.2 端末フィルタ

(1) 端末フィルタの概要

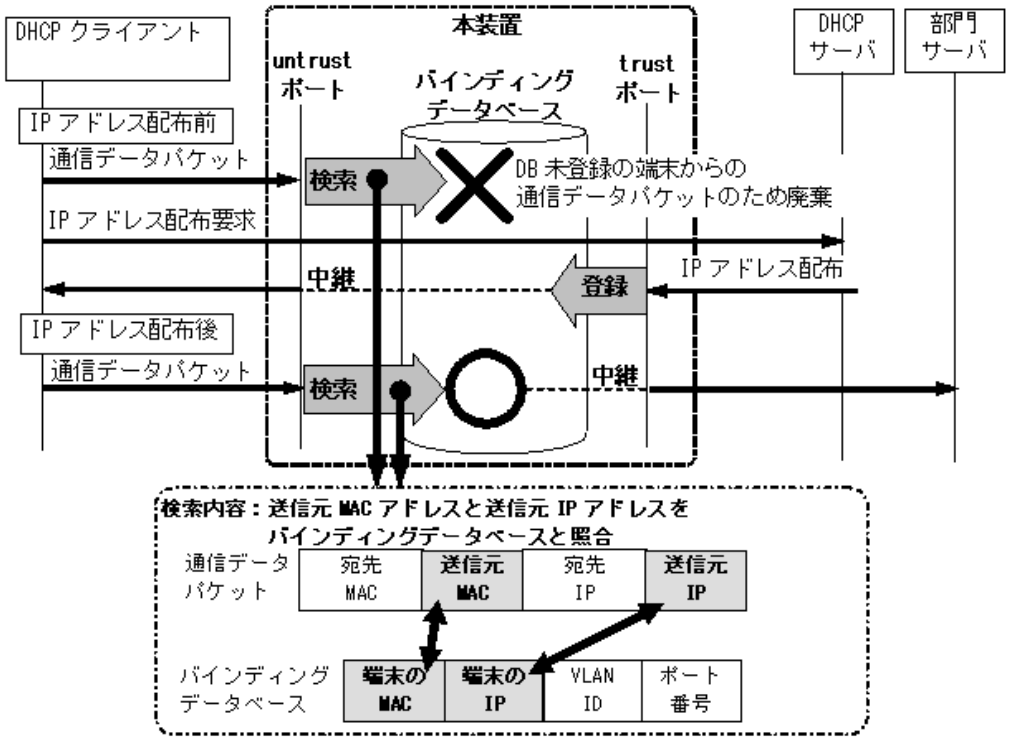
端末フィルタは，DB 未登録の端末からの通信データパケットをすべて廃棄します。端末フィルタの対象は，untrust ポートに接続された端末からの通信データパケットです。

端末フィルタを有効にする際，フィルタ条件を設定します。フィルタ条件は下記の 3 種類がありますので，セキュリティポリシーに従って設定してください。

- 送信元 IP アドレス（Source IP Address）だけの端末フィルタ
- 送信元 IP アドレス（Source IP Address）と送信元 MAC アドレス（Source MAC Address）の端末フィルタ
- 送信元 MAC アドレス（Source MAC Address）だけの端末フィルタ

端末フィルタは，コンフィグレーションコマンド ip verify source でポート単位に設定してください。

図 18-5 端末フィルタの動作概要（送信元 IP アドレスと送信元 MAC アドレスの端末フィルタ例）



これにより，バインディングデータベースに未登録の送信元 IP ドレスと送信元 MAC アドレスのパケットを廃棄します。

（2） 固定 IP アドレス端末の通信許可

untrust ポートに接続された固定 IP アドレスを持つ部門サーバなどの通信を許可する場合，バインディングデータベースに端末情報をスタティック登録することで通信を許可できます。

固定 IP アドレス端末の通信許可は，コンフィグレーションコマンド ip source binding で，下記の情報を登録してください。

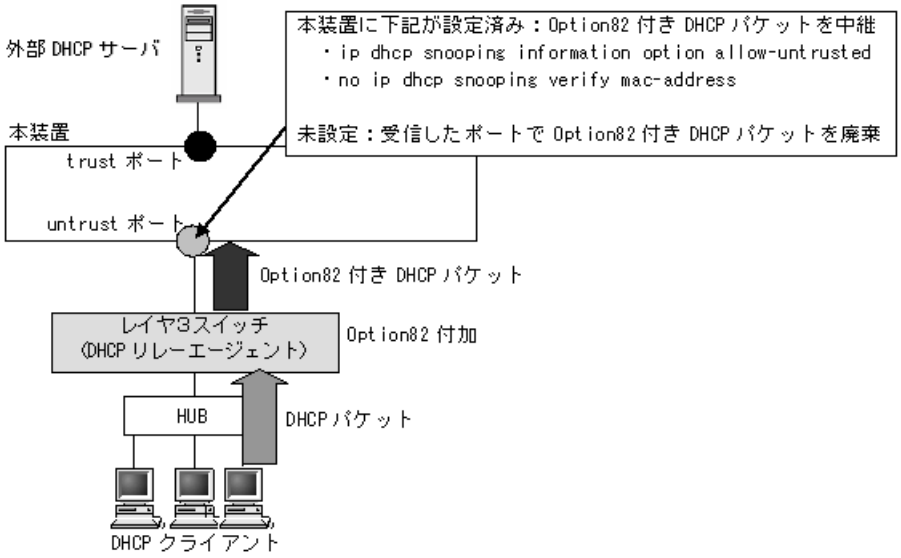
- 端末の IP アドレス
- 端末の MAC アドレス
- 端末を接続するポート番号またはチャネルグループ番号
- 端末を接続するポートまたはチャネルグループの所属する VLAN ID

本コマンドでの設定可能エントリ数については，「表 18-2　バインディングデータベースの登録内容」を参照してください。

18.1.3　DHCP の Option82 付きパケットの中継

本装置と DHCP クライアントの間に，レイヤ 3 スイッチなど DHCP リレーエージェントを配置した構成の場合，DHCP リレーエージェントが DHCP クライアントからの DHCP パケットに Option82 情報を付加する場合があります。

図 18-6　Option82 付きパケットが付加される構成例



Option82 付きパケットは，DHCP リレーエージェントが DHCP クライアントの拡張情報を伝達するための情報で，端末 MAC アドレス，接続ポート番号，ホスト名などが含まれます。

DHCP snooping を有効にした場合，untrust ポートで受信した Option82 付きパケットは廃棄します。従って，本装置が DHCP サーバと DHCP リレーエージェントの中間に配置され，DHCP リレーエージェントが Option82 情報を付加する構成の場合，本装置の DHCP snooping が正しく動作できません。

この場合，コンフィグレーションコマンド ip dhcp snooping information option allow-untrusted で，Option82 付きパケットの通信許可を設定します。

また，DHCP snooping は，untrust ポートから受信した DHCP パケットの送信元 MAC アドレスと

DHCP パケット内のクライアントハードウェアアドレスの一致（MAC アドレスの整合性）を確認しています。untrust ポートに DHCP リレーエージェントが存在した場合，パケットの送信元 MAC アドレスが書き換えられるため，本装置は DHCP パケットを不正と判断し廃棄します。

このため，Option82 付きパケット通信許可設定と共に，コンフィグレーションコマンド no ip dhcp snooping verify mac-address で，MAC アドレス整合性チェックの解除が必要です。

18.1.4 DHCP パケットの受信レート制限

DHCP snooping 有効時に，受信する DHCP パケットの監視を実施する際，設定した受信レートを超えた DHCP パケットを廃棄する機能です。

受信レートはコンフィグレーションコマンド ip dhcp snooping limit rate で設定できます。本コマンド未設定の場合は，受信レートは無制限となります。

DHCP パケットの受信レート制限は，untrust ポートだけを対象とし，trust ポートは対象外です。

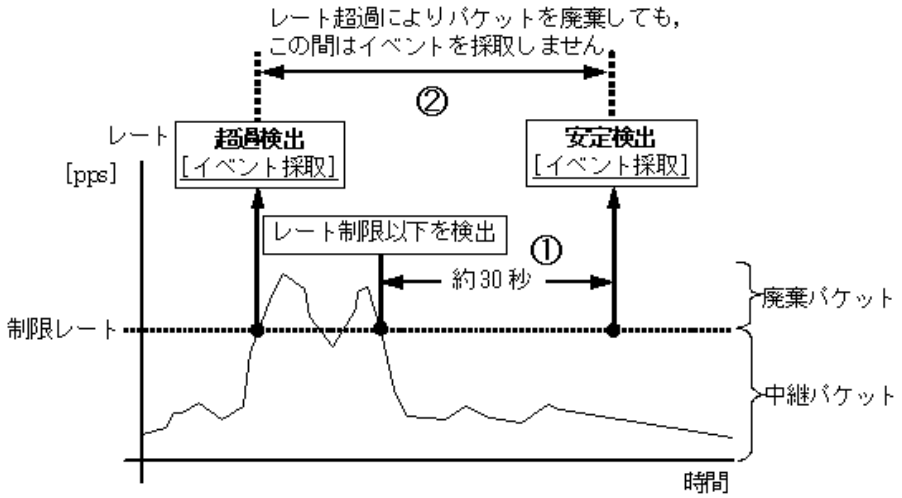
受信レートを超えた DHCP パケットは廃棄し，イベントトレース情報を採取します。ただし，Trap は発行しません。なお，イベントトレース情報は運用コマンド show event-trace で，廃棄パケット数については運用コマンド show ip dhcp snooping statistics で確認してください。

イベントトレース情報は下記の契機で採取します。

- コンフィグレーションで設定した受信レートを超過したときに，「超過検出」イベントを採取します。
- 「超過検出」イベントを採取後，設定レート制限以下の状態が約 30 秒間継続（図内①）したときに，「安定検出」イベントを採取します。
  「超過検出」イベントを採取後から「安定検出」イベント採取までの間（図内②）は，レート超過によりパケットを廃棄してもイベントを採取しません。

イベントトレース情報の採取契機を次の図に示します。

図 18-7 DHCP パケット受信レートのイベントトレース情報採取契機



18.1.5　ダイナミック ARP 検査機能

DHCP snooping 有効時に，本装置が untrust ポートで受信した ARP パケット内の発信者 IP アドレス（Sender IP Address）および発信者 MAC アドレス（Sender MAC Address）が，バインディングデータベースに登録されている正規端末のアドレスであるか検査する機能です。本機能により，DB 未登録の端末から送信された詐称 ARP パケットによる，正規端末の通信の乗っ取りを防止します。

（1）ダイナミック ARP 検査対象

ダイナミック ARP 検査の対象は，下記の条件にすべて一致する ARP パケットです。

- ARP 検査対象 VLAN に所属するポートで受信した ARP パケット
  （ARP 検査対象 VLAN は，コンフィグレーションコマンド ip arp inspection vlan で設定します。）
- untrust ポート（コンフィグレーションコマンド ip arp inspection trust を設定していないポート）で受信した ARP パケット

（2）ダイナミック ARP 検査の基本検査

基本検査では，untrust ポートで受信した ARP パケットとバインディングデータベースのエントリの整合性を検査します。

ダイナミック ARP 検査の基本検査を下記に示します。

図 18-8　ダイナミック ARP 検査の基本検査概要

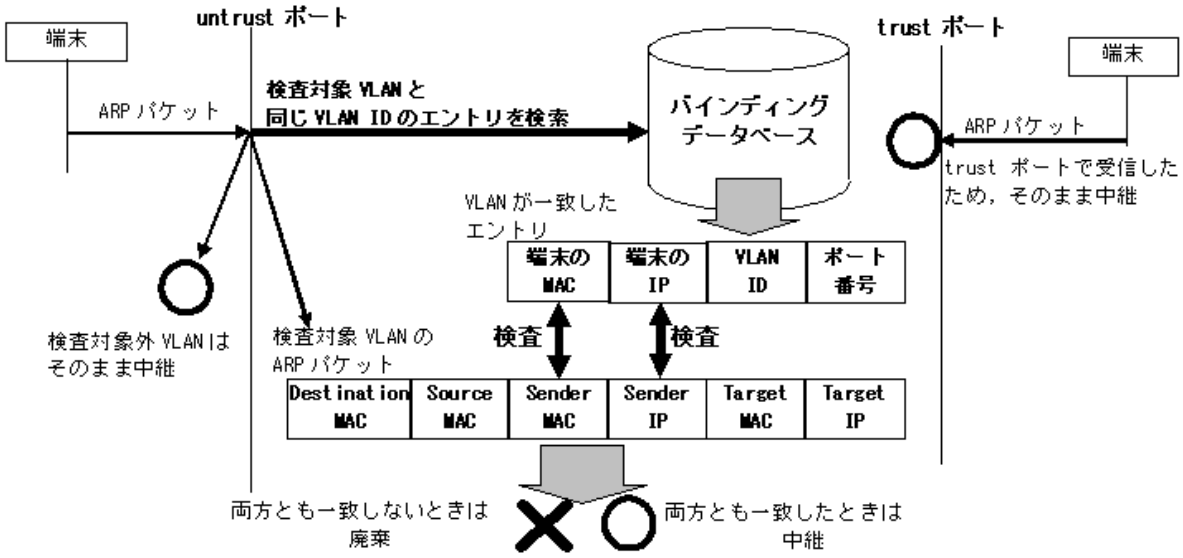


表 18-3　ARP パケットのフィールド別基本検査対象

ARP パケットのフィールド			Request	Reply	備考
Ethernet ヘッダ	Destination	MAC	－	－	－
	Source	MAC	－	－	－
ARP ヘッダ	Sender	MAC	○	○	バインディングデータベースと比較
		IP	○	○	バインディングデータベースと比較

ARP パケットのフィールド			Request	Reply	備考
	Target	MAC	−	−	−
		IP	−	−	−

（凡例）

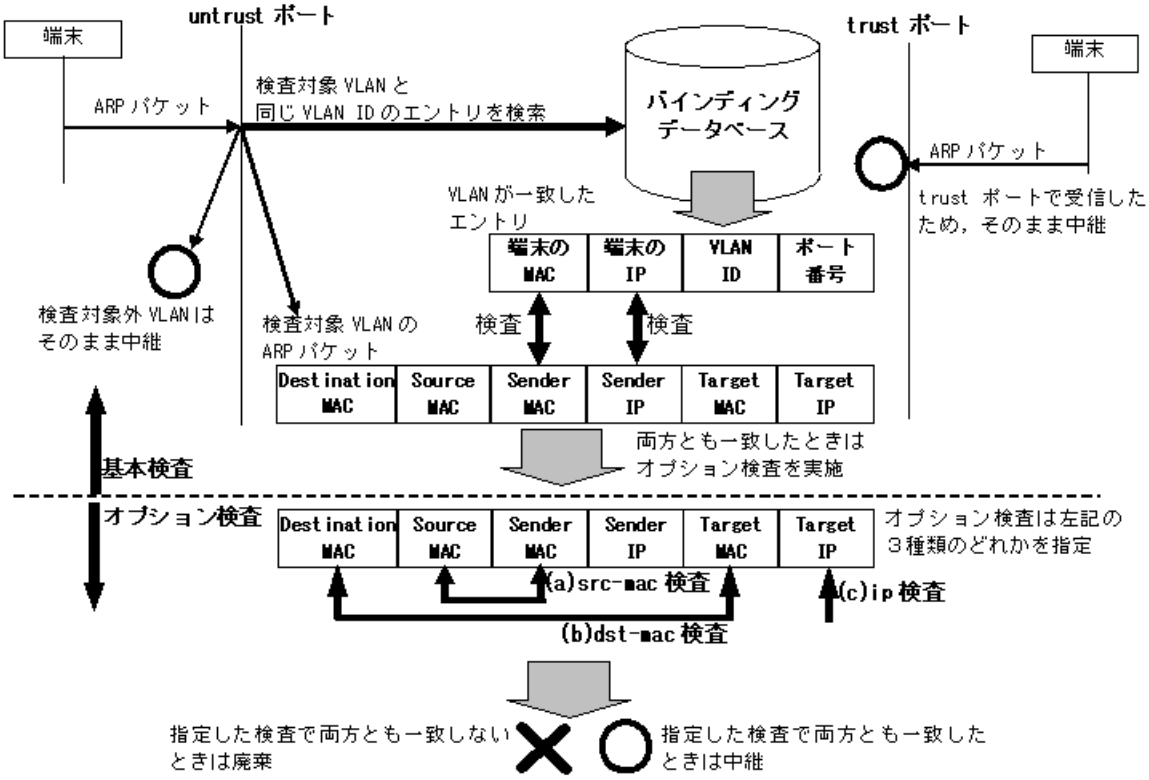
○：検査対象

−：検査対象外

（3） ダイナミック ARP 検査のオプション検査

ダイナミック ARP 検査機能は，バインディングデータベースとの整合性を検査しますが，オプションとして ARP パケット内データの整合性の検査もサポートします。

図 18-9　ダイナミック ARP 検査の基本検査とオプション検査の関係



（a） 送信元 MAC アドレス指定 (src-mac 検査）

受信 ARP パケットの送信元 MAC アドレス（Source MAC Address）と，発信者 MAC アドレス（Sender MAC Address）が同一であることを検査します。

ARP Request，ARP Reply の双方に対して実施します。

（b） 宛先 MAC アドレス指定（dst-mac 検査）

受信 ARP パケットの宛先 MAC アドレス（Destination MAC Address）と，対象者 MAC アドレス（Target MAC Address）が同一であることを検査します。

ARP Reply に対してだけ実施します。

(c) IP アドレス指定（ip 検査）

受信 ARP パケットの対象者 IP アドレス（Target IP Address）が，下記の範囲内であることを検査します。

- 1.0.0.0 ～ 126.255.255.255
- 128.0.0.0 ～ 223.255.255.255

ARP Reply に対してだけ実施します。

表 18-4　ARP パケットのフィールド別オプション検査対象

ARP パケットのフィールド			src-mac 検査		dst-mac 検査		ip 検査	
			Request	Reply	Request	Reply	Request	Reply
Ethernet ヘッダ	Destination	MAC	－	－	－	○	－	－
	Source	MAC	○	○	－	－	－	－
ARP ヘッダ	Sender	MAC	○	○	－	－	－	－
		IP	－	－	－	－	－	－
	Target	MAC	－	－	－	○	－	－
		IP	－	－	－	－	－	○

（凡例）
○：検査対象
－：検査対象外

(4) ARP パケットの受信レート制限

ダイナミック ARP 検査機能有効時に，ダイナミック ARP 検査対象 VLAN に所属するポートで，設定した受信レートを超えた ARP パケットを廃棄する機能です。

受信レートはコンフィグレーションコマンド ip arp inspection limit rate で設定できます。本コマンド未設定の場合は，受信レートは無制限となります。

受信レートを超えた ARP パケットは廃棄し，イベントトレース情報を採取します。ただし，Trap は発行しません。なお，イベントトレース情報は運用コマンド show event-trace で，廃棄パケット数については運用コマンド show ip arp inspection statistics で確認してください。

ARP パケット受信レート超過時のイベントトレース情報の採取契機は，DHCP パケットの受信レート制限と同様です。「18.1.4　DHCP パケットの受信レート制限図 18-7　DHCP パケット受信レートのイベントトレース情報採取契機」を参照してください。

18.1.6　バインディングデータベースの保存

コンフィグレーションで指定することにより，バインディングデータベースの保存，および装置再起動時の復元が可能です。

(1) バインディングデータベースの保存の動作条件

バインディングデータベースの保存は，下記のコンフィグレーションコマンドの設定により動作可能です。

- ip dhcp snooping：DHCP snooping の有効設定
- ip dhcp snooping vlan：DHCP snooping を実施する VLAN の設定

- ip dhcp snooping database url：バインディングデータベース保存先

本装置では，書き込み指定時間満了時または特定オペレーションにより保存を実施します。

(2) 書き込み指定時間満了時の保存

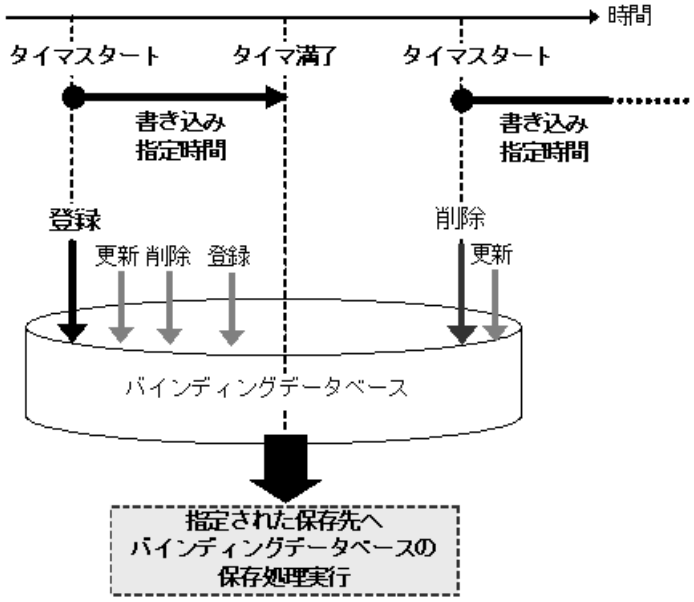
書き込み指定時間は下記のいずれかを保存契機としてタイマをスタートし，タイマが満了した場合に指定した保存先へ保存します。

- ダイナミックのバインディングデータベースの登録・更新・削除時
- コンフィグレーションコマンド ip dhcp snooping database url 設定時（保存先の変更を含む）
- 運用コマンド clear ip dhcp snooping binding 実行時

書き込み指定時間は，コンフィグレーションコマンド ip dhcp snooping database write-delay で設定します。

書き込み指定時間のタイマは，上記の保存契機でスタートすると，タイマ満了となるまではタイマを停止しません。この間にバインディングデータベースの登録・更新・削除が発生してもタイマの再スタートはありません。

図 18-10　保存契機と書き込み指定時間の動作概要（バインディングデータベース登録を契機とした例）



(3) 特定オペレーションによる保存

装置再起動を促す下記のオペレーションを実行した場合は，その時点でのバインディングデータベースをコンフィグレーションで指定した保存先へ保存します。

なお，コンフィグレーションで保存先が指定されていない場合は，下記のオペレーションを実行しても，バインディングデータベースを保存しません。

表 18-5　特定オペレーションによる保存

オペレーション	保存先	動作契機
reload	コンフィグレーションで指定した保存先	運用端末から運用コマンド入力
ppupdate		運用端末から運用コマンド入力
backup		運用端末から運用コマンド入力
copy-config		OAN から実行

（4） バインディングデータベースの保存先

コンフィグレーションで指定するバインディングデータベースの保存先は，内蔵フラッシュメモリと MC があります。どちらの場合も書き込み実施時の全エントリが保存され，次の書き込み実施時に上書きされます。

保存先は，コンフィグレーションコマンド ip dhcp snooping database url で設定します。

（5） 保存したバインディングデータベースの復元

保存したバインディングデータベースは，装置起動時に復元します。装置起動前に下記を確認してください。

- コンフィグレーションコマンド ip dhcp snooping database url で保存先が設定されている
- 保存先が MC の場合，保存したファイルの MC が挿入されている

18.1.7　DHCP snooping 使用時の注意事項

（1） 運用前のシステムファンクションリソース設定について

DHCP snooping を使用する場合，システムファンクションリソースの設定が必要となります。システムファンクションリソース設定については，「9.1.6　システムファンクションリソース配分の設定」を参照し，DHCP snooping 以外の適切な機能も合わせて選択してください。

（2） レイヤ 2 認証機能との併用

DHCP snooping および端末フィルタと，各認証機能（IEEE802.1X 認証，Web 認証，MAC 認証）は，同一ポート内での併用が可能です。

この場合，端末フィルタよりも各認証の結果が優先されるため，端末フィルタで通信許可された端末においても，各認証機能で許可されなければ通信できません。

また，trust ポート，untrust ポートに依存せず各認証機能は混在可能です。

DHCP snooping とレイヤ 2 認証機能を併用した場合，通信可能な最大端末数は DHCP snooping の管理端末数（最大 246 台）となります。

（3） ダイナミック ARP 検査機能の使用について

ダイナミック ARP 検査機能は，下記の DHCP snooping を設定し，バインディングデータベースが生成されることが必要です。

- コンフィグレーションコマンド ip dhcp snooping：DHCP snooping の有効設定
- コンフィグレーションコマンド ip dhcp snooping vlan；DHCP snooping を実施する VLAN の設定

また，コンフィグレーションコマンド ip source binding でバインディングデータベースにスタティック登

録されたエントリもダイナミック ARP 検査の対象となります。

（4）バインディングデータベースの保存と復元について

- コンフィグレーションコマンド ip dhcp snooping database url 未設定（初期状態）の場合，バインディングデータベースは保存されません。装置を再起動すると登録済のバインディングデータベースが消去されるため，DHCP クライアントからの通信ができなくなります。この場合は，DHCP クライアント側で IP アドレスの解放と更新を実施してください。（例：Windows の場合，コマンドプロンプトから ipconfig /release を実行した後に，ipconfig /renew を実行してください。）
  これにより，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 クライアントの通信が可能になります。
- 復元するエントリのうち，DHCP サーバのリース時間を満了したエントリは復元されません。バインディングデータベースが保存された後，本装置の電源 OFF 前に時計設定を変更すると，電源 ON 後のバインディングデータベース復元処理が正しく実施されない場合があります。
- コンフィグレーションコマンド ip source binding によりスタティック登録されたエントリの復元は，起動時のスタートアップコンフィグレーションファイルに従います。
- バインディングデータベースの保存先を MC にした場合は，装置再起動後の画面にプロンプトが表示されるまで MC を抜かないでください。
- 運用コマンド backup で保存して運用コマンド restore で復元する場合，復元先の装置にコンフィグレーションコマンド ip dhcp snooping database url が設定されていないことを確認してから実行してください。設定されたまま運用コマンド restore を実行すると，バインディングデータベース復元処理が正しく実施されない場合があります。

18.2 DHCP snooping 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

DHCP 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 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
ip arp inspection limit rate	当該ポートでの ARP パケットの受信レート（1 秒あたりに受信可能な ARP パケット数）を設定します。
ip arp inspection trust	ダイナミック ARP 検査を実施しないポートに対して設定します。
ip arp inspection validate	ダイナミック ARP 検査機能有効時に，ダイナミック ARP 検査の精度を高めるために追加する検査項目を設定します。
ip arp inspection vlan	ダイナミック ARP 検査機能の検査対象 VLAN を設定します。
ip dhcp snooping	DHCP snooping の有効／無効を設定します。
ip dhcp snooping database url	バインディングデータベースの保存先を設定します。
ip dhcp snooping database write-delay	バインディングデータベース保存時の書き込み指定時間を設定します。
ip dhcp snooping information option allow-untrusted	untrust ポートでの Option82 付きの DHCP パケットの受信可否を設定します。
ip dhcp snooping limit rate	当該ポートでの DHCP パケットの受信レート（1 秒あたりに受信可能な DHCP パケット数）を設定します。
ip dhcp snooping trust	インタフェースを trust ポートとして設定します。
no ip dhcp snooping verify mac-address	untrust ポートから受信した DHCP パケットの送信元 MAC アドレスと，クライアントのハードウェアアドレスの一致をチェックするか否かを設定します。
ip dhcp snooping vlan	VLAN での DHCP snooping を有効にします。
ip source binding	固定 IP アドレス端末用のバインディングデータベースを設定します。
ip verify source	DHCP snooping バインディングデータベースを基に，端末フィルタを実施する場合に設定します。

18.2.2 DHCP snooping のコンフィグレーションを設定する前に

(1) システムファンクションリソース割り当ての設定

DHCP snooping を設定する場合は，コンフィグレーションを設定する前に，下記を設定してください。

［設定のポイント］

DHCP snooping を使用するには，設定の最初の段階でシステムファンクションリソースの割り当てをコンフィグレーションで設定する必要があります。システムファンクションリソースの割り当て設定は装置の再起動が必要です。システムファンクションリソースの割り当てについては「9.1.6 システムファンクションリソース配分の設定」を参照してください。
本例ではフィルタと DHCP snooping を割り当てます。

［コマンドによる設定］

1. **(config)# system function filter dhcp-snooping**
```
Please execute the reload command after save,
```

```
because this command becomes effective after reboot.
```

システムファンクションリソースとしてフィルタと DHCP snooping を割り当てます。

2. **(config)# end**

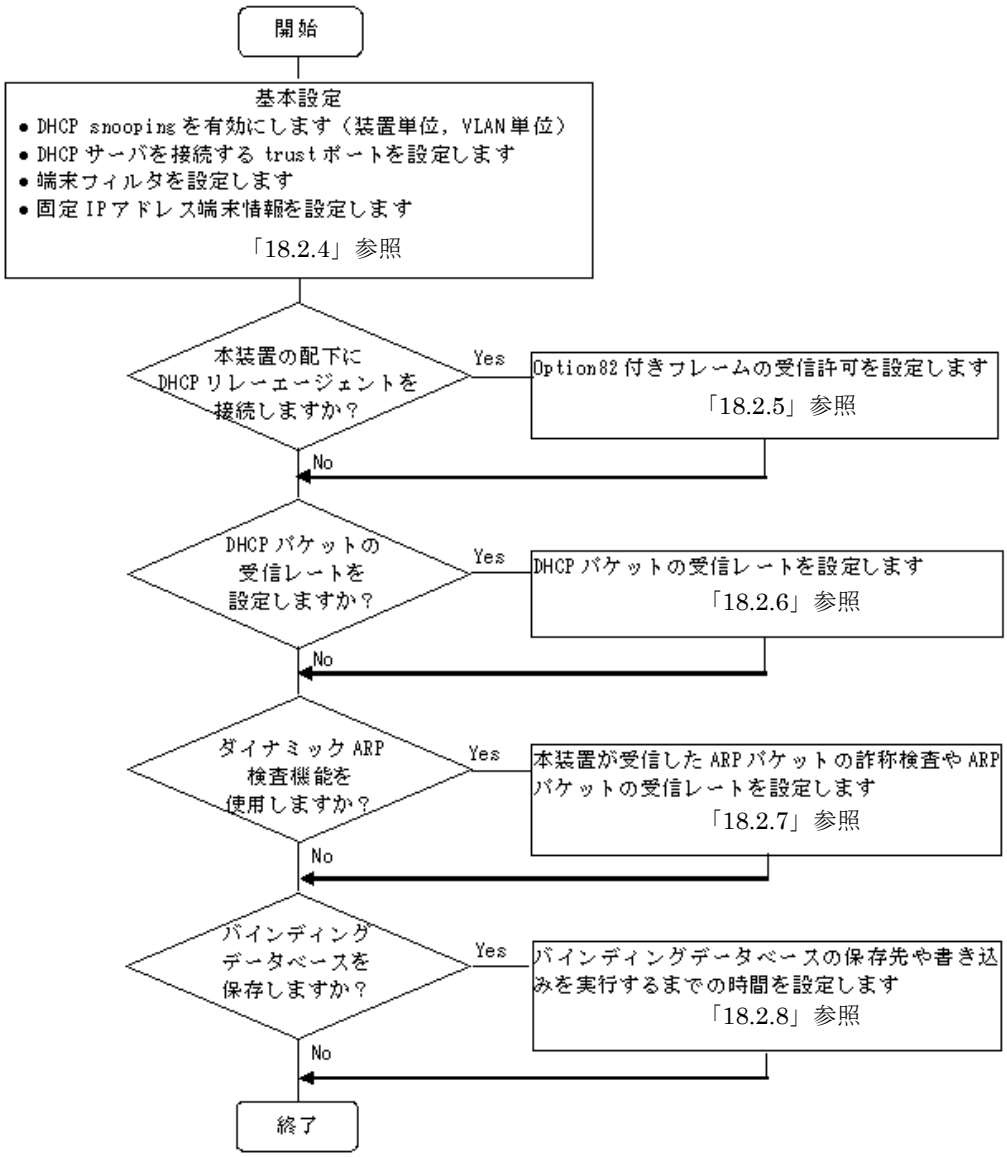
```
# copy running-config startup-config
Do you wish to copy from running-config to startup-config? (y/n): y
@# reload
Restart OK? (y/n): y
```

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，装置を再起動してください。

18.2.3 DHCP snooping の設定手順

本節の設定例は，レイヤ３スイッチを経由した構成例を基本設定とし，DHCP snooping の各機能を設定する形態で記載しています。次の図に示す手順に沿って設定してください。

図 18-11 DHCP snooping の設定手順

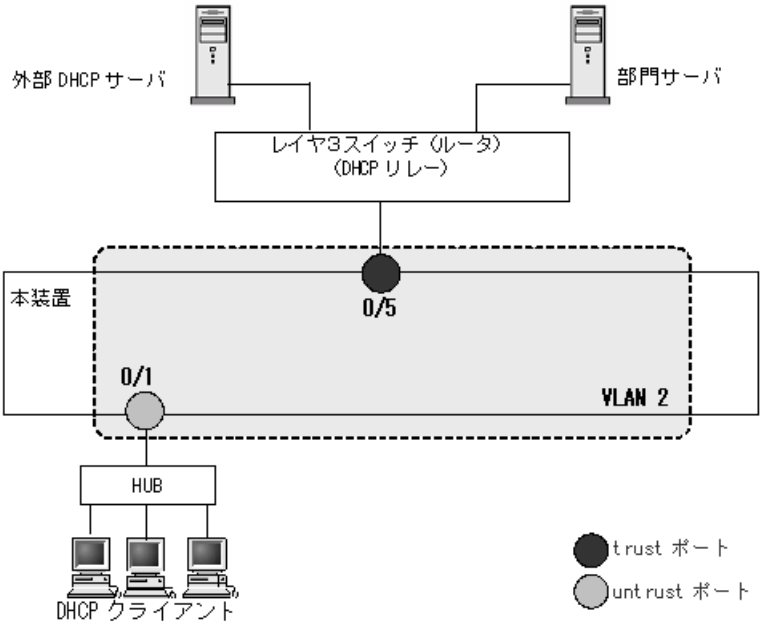


18.2.4 基本設定（レイヤ３スイッチを経由した場合）

DHCP snooping を使用するための基本的な設定について説明します。

DHCP サーバと部門サーバをレイヤ３スイッチを経由する構成で，レイヤ３スイッチに接続するポートを trust ポートとして設定します。

図 18-12 レイヤ３スイッチ経由の構成例



（1） DHCP snooping の有効設定

［設定のポイント］

装置としての DHCP snooping を有効にし，下記を設定します。

- DHCP snooping を有効にする VLAN を設定
- DHCP サーバを接続するポートを trust ポートとして設定
- untrust ポートに，DB 未登録の端末からのパケットを廃棄する端末フィルタを設定

［コマンドによる設定］

1. **(config)# ip dhcp snooping**
   装置としての DHCP snooping 機能を有効にします。
2. **(config)# vlan 2**
   (config-vlan)# exit
   (config)# ip dhcp snooping vlan 2
   VLAN ID 2 で DHCP snooping を有効にします。本コマンドを指定しない VLAN では DHCP snooping は動作しません。
3. **(config)# interface fastethernet 0/1**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 2
   (config-vlan)# exit
   ポート 0/1 をアクセスポートとし，ポート 0/1 が所属する VLAN として VLAN ID 2 を設定します。

(2) trust ポートの設定

[設定のポイント]

DHCP サーバに接続するポート（構成図ではレイヤ 3 スイッチと接続するポート）を trust ポートとして使用するインタフェースを設定します。

[コマンドによる設定]

1. **(config)# interface fastethernet 0/5**
   (config-if)# ip dhcp snooping trust
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 2
   (config-if)# exit
   ポート 0/5 を trust ポートとして設定します。その他のポートは untrust ポートとなります。またポート 0/5 をアクセスポートとし，ポート 0/5 が所属する VLAN として VLAN ID 2 を設定します。

(3) 端末フィルタの設定

[設定のポイント]

バインディングデータベースを基にパケットを廃棄するポートに端末フィルタを設定します。

[コマンドによる設定]

1. **(config)# interface fastethernet 0/1**
   (config-if)# ip verify source port-security
   (config-if)# exit
   ポート 0/1 に送信元 IP アドレスと送信元 MAC アドレスの端末フィルタを設定します。

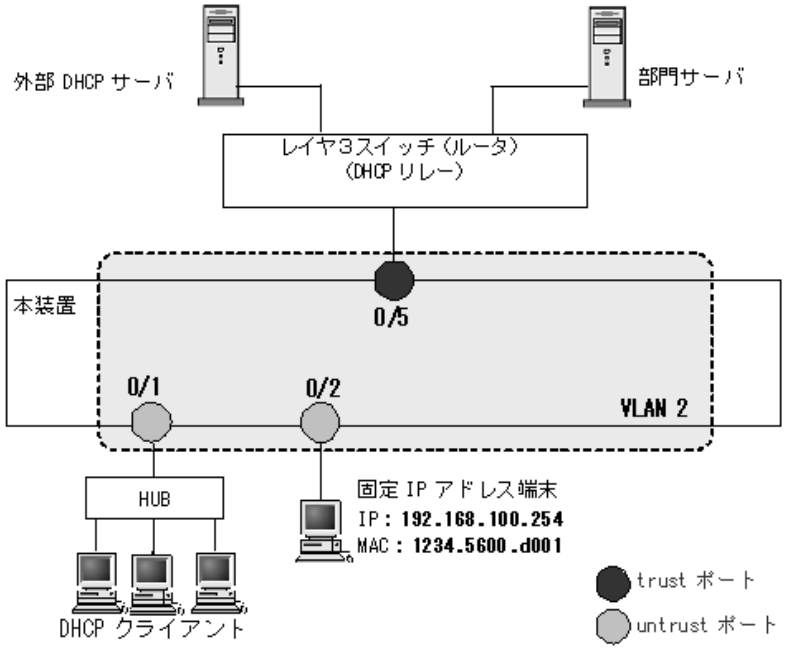
[注意事項]

trust ポートで本コマンドを設定しても，端末フィルタは無効です。また，DHCP snooping 有効時は，ip dhcp snooping vlan で設定されていない VLAN でも端末フィルタが有効となりますのでご注意ください。

(4) 固定 IP アドレス端末を接続した場合

固定 IP アドレスを持つ端末を接続する場合の設定について説明します。

図 18-13　固定 IP アドレス端末を接続した場合の構成例



DHCP snooping の設定は「18.2.4　基本設定（レイヤ 3 スイッチを経由した場合)」と同様です。本例では，固定 IP アドレスを持つ端末を untrust ポートに接続するため，バインディングデータベースに固定 IP アドレス端末の登録が必要です。

上記の設定は，コンフィグレーションコマンドで設定します。

［設定のポイント］

固定 IP アドレスを持つ端末用にバインディングデータベースを設定します。

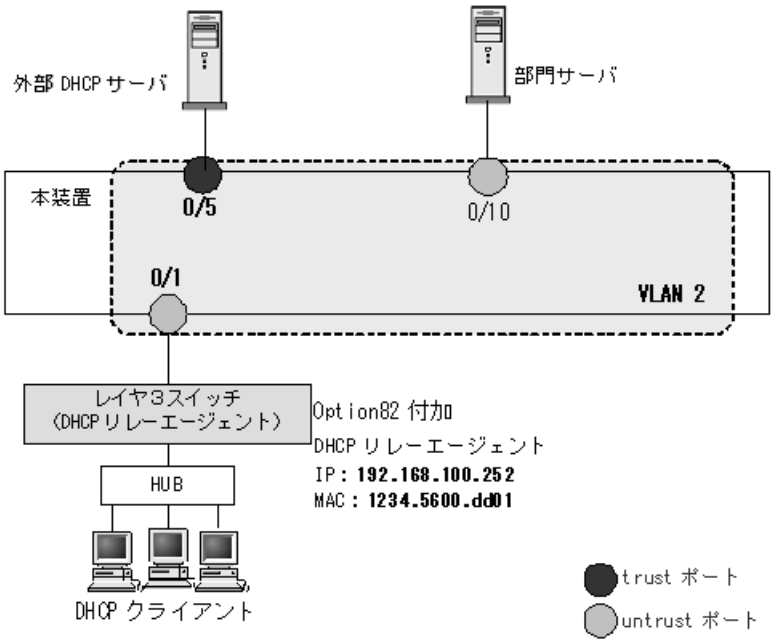
［コマンドによる設定］

1. **(config)# interface fastethernet 0/2**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 2
   (config-if)# exit
   固定 IP アドレス端末を接続するポート 0/2 に VLAN ID 2 を設定します。
2. **(config)# ip source binding 1234.5600.d001 vlan 2 192.168.100.254 interface fastethernet 0/2**
   端末の MAC アドレス，端末が接続されている VLAN ID，端末の IP アドレス，端末が接続されているポート番号を，バインディングデータベースに設定します。

18.2.5　本装置の配下に DHCP リレーエージェントが接続された場合

本装置の配下に Option82 を付加した DHCP パケットを送信する DHCP リレーエージェントを接続した場合，本装置で Option82 付きパケットを中継できるように設定します。

図 18-14　本装置の配下に DHCP リレーエージェントを接続した場合の構成例



本装置の DHCP snooping 設定は「18.2.4　基本設定（レイヤ 3 スイッチを経由した場合)」同様です。本例では，DHCP リレーエージェントが Option82 付き DHCP パケットを送信するため，本装置で DHCP リレーエージェントを接続する untrust ポートで Option82 付きパケットの中継を許可する設定が必要です。その他，同じ untrust ポートで DHCP パケットの送信元アドレスをチェックしない設定，ARP パケットの中継を許可する設定，端末フィルタを IP アドレスだけでフィルタする設定も必要です。

上記の設定は，コンフィグレーションコマンドで設定します。

（1） Option82 付きパケットを untrust ポートで受信許可する設定

[設定のポイント]

untrust ポートでの Option82 付き DHCP パケットを受信可能に設定します。

[コマンドによる設定]

1. **(config)# ip dhcp snooping information option allow-untrusted**
   untrust ポートで Option82 付きの DHCP パケットの受信を許可します。

（2） untrust ポートで DHCP パケットの送信元アドレスチェックを解除する設定

[設定のポイント]

untrust ポートで DHCP パケットの送信元 MAC アドレスをチェックしないで中継するため，アドレスチェック機能の解除を設定します。

[コマンドによる設定]

1. **(config)# no ip dhcp snooping verify mac-address**
   untrust ポートで受信した DHCP パケットの送信元 MAC アドレスのチェック無を設定します。

[注意事項]

本コマンド未設定の場合，送信元 MAC アドレスをチェックするため，untrust ポートに DHCP リレーエージェントを接続できなくなります。

（3） untrust ポートで ARP パケットの中継を許可するバインディングデータベースの設定

［設定のポイント］

untrust ポートに接続した DHCP リレーエージェントからの ARP パケットを中継するために，DHCP リレーエージェントのアドレスをバインディングデータベースに設定します。

［コマンドによる設定］

1. **(config)# ip source binding 1234.5600.dd01 vlan 2 192.168.100.252 interface fastethernet 0/1**

   DHCP リレーエージェントの MAC アドレス，接続されている VLAN ID，IP アドレス，接続されているポート番号を，バインディングデータベースとして設定します。

（4） untrust ポートで IP アドレスだけの端末フィルタの設定

［設定のポイント］

DHCP クライアントからのパケットは，レイヤ 3 スイッチ経由により送信元 MAC アドレスが書き換えられているため，untrust ポートに IP アドレスだけの端末フィルタを設定します。

［コマンドによる設定］

1. **(config)# interface fastethernet 0/1**
   (config-if)# ip verify source
   (config-if)# exit

   ポート 0/1 に IP アドレスだけの端末フィルタを設定します。

18.2.6 DHCP パケットの受信レートの設定

DHCP パケットを受信するポートの受信レート制限をコンフィグレーションで設定します。

DHCP snooping の設定は「18.2.4 基本設定（レイヤ 3 スイッチを経由した場合）」と同様です。

（1） 受信レートの設定

［設定のポイント］

端末から DHCP パケットを受信するポート 0/1 に受信レートを設定します。

［コマンドによる設定］

1. **(config)# interface fastethernet 0/1**
   (config-if)# ip dhcp snooping limit rate 50
   (config-if)# exit

   ポート 0/1 の受信レートを 50 パケット / 秒に設定します。

18.2.7 ダイナミック ARP 検査機能の設定

ダイナミック ARP 検査機能を使用するための基本的な設定について説明します。

DHCP snooping の設定は「18.2.4 基本設定（レイヤ 3 スイッチを経由した場合)」と同様です。

(1) ダイナミック ARP 検査機能の検査対象 VLAN の設定（基本検査対象）

[設定のポイント]

DHCP snooping を有効にした VLAN のうちで，ダイナミック ARP 検査機能の検査対象 VLAN ID を設定します。設定した VLAN で受信した ARP パケットが基本検査対象となります。

[コマンドによる設定]

1. **(config)# ip arp inspection vlan 2**
   VLAN ID 2 をダイナミック ARP 検査対象に設定します。本コマンドを指定しない VLAN ではダイナミック ARP 検査機能は動作しません。

[注意事項]

1. コンフィグレーションコマンド ip dhcp snooping vlan で設定している VLAN ID を指定してください。
2. 本コマンドを設定した場合は，コンフィグレーションコマンド ip source binding で登録したバインディングデータベースエントリも，ダイナミック ARP 検査の対象となります。
3. 本コマンドを設定した VLAN に所属しているポートに対して，コンフィグレーションコマンド ip arp inspection trust を設定した場合は，そのポートでダイナミック ARP 検査を実施しません。

(2) ダイナミック ARP 検査を実施しないポートの設定

[設定のポイント]

ダイナミック ARP 検査を実施しないポートに対して設定します。

[コマンドによる設定]

1. **(config)# interface fastethernet 0/5**
   (config-if)# ip arp inspection trust
   (config-if)# exit
   ポート 0/5 はダイナミック ARP 検査を実施しないポートとなります。その他のポートはダイナミック ARP 検査を実施するポートとなります。

[注意事項]

1. 本コマンドを設定したポートでは，ダイナミック ARP 検査機能の検査対象 VLAN に所属していても，ダイナミック ARP 検査を実施しません。
2. 本コマンドを設定したポートの ARP パケット受信レートは無制限となります。

(3) ダイナミック ARP 検査機能のオプション検査の設定

[設定のポイント]

基本検査した ARP パケットに対するオプション検査を設定します。本例では，受信 ARP パケットの送信元 MAC アドレス（Source MAC Address）と，発信者 MAC アドレス（Sender MAC Address）が同一であることを検査するよう設定します。

［コマンドによる設定］

1. **(config)# ip arp inspection validate src-mac**
   受信 ARP パケットの送信元 MAC アドレス（Source MAC Address）と，発信者 MAC アドレス（Sender MAC Address）が同一であることを検査する src-mac 検査を設定します。

（4） ARP パケットの受信レートの設定

［設定のポイント］
端末から ARP パケットを受信するポート 0/1 に受信レートを設定します。

［コマンドによる設定］

1. **(config)# interface fastethernet 0/1**
   (config-if)# ip arp inspection limit rate 100
   (config-if)# exit
   ポート 0/1 の受信レートを 100 パケット / 秒に設定します。

18.2.8 バインディングデータベース保存の設定

（1） 保存先の設定

（a） 内蔵フラッシュメモリに保存する場合

［設定のポイント］
バインディングデータベースの保存先に内蔵フラッシュメモリを設定します。

［コマンドによる設定］

1. **(config)# ip dhcp snooping database url flash**
   保存先として内蔵フラッシュメモリを設定します。

［注意事項］

運用コマンド backup を実行した場合，内蔵フラッシュメモリに保存されたバインディングデータベースもバックアップ対象となります。運用コマンド restore で復元できます。

（b） MC に保存する場合

［設定のポイント］
バインディングデータベースの保存先に MC を設定します。MC の場合は保存するファイル名を設定できます。

［コマンドによる設定］

1. **(config)# ip dhcp snooping database url mc dhcpsn-db**
   保存先として MC，および保存時のファイル名 dhcpsn-db を設定します。

［注意事項］

保存先を MC にする場合は，本装置のメモリカードスロットに MC を挿入しておいてください。また，MC はアラクサラ製品（AX-F2430-SD128）をご使用ください。

（2） 書き込み指定時間の設定

［設定のポイント］
バインディングデータベースの保存先への書き込み指定時間を設定します。

［コマンドによる設定］

1. **(config)# ip dhcp snooping database write-delay 3600**
   下記のいずれかを保存契機とし，保存処理を実行するまでの時間を 3600 秒に設定します。
   - ダイナミックのバインディングデータベースの登録・更新・削除時
   - コンフィグレーションコマンド ip dhcp snooping database url 設定時（保存先の変更を含む）
   - 運用コマンド clear ip dhcp snooping binding 実行時

［注意事項］

次回の保存契機から本コマンドで設定した時間が運用に反映されます。

18.3 DHCP snooping のオペレーション

18.3.1 運用コマンド一覧

DHCP snooping の運用コマンド一覧を次の表に示します。

表 18-7 運用コマンド一覧

コマンド名	説明
show ip arp inspection statistics	ダイナミック ARP 検査の統計情報を表示します。
clear ip arp inspection statistics	ダイナミック ARP 検査の統計情報をクリアします。
show ip dhcp snooping	DHCP snooping 情報を表示します。
show ip dhcp snooping binding	DHCP snooping バインディングデータベース情報を表示します。
clear ip dhcp snooping binding	DHCP snooping バインディングデータベース情報をクリアします。
show ip dhcp snooping statistics	DHCP snooping 統計情報を表示します。
clear ip dhcp snooping statistics	DHCP snooping 統計情報をクリアします。

18.3.2 DHCP snooping の確認

(1) DHCP snooping 情報の確認

DHCP snooping 情報を運用コマンド show ip dhcp snooping で表示します。Option82 付きパケットの許可状態，DHCP パケット送信元 MAC アドレスのチェック可否，DHCP snooping が動作している VLAN リスト情報などを表示します。

運用コマンド show ip dhcp snooping の実行結果を次の図に示します。

図 18-15 show ip dhcp snooping の実行結果

```
> show ip dhcp snooping

Date 2007/12/12 16:34:10 UTC
Switch DHCP snooping is Enable
Option allow untrusted: off,  Verify mac-address: on
DHCP snooping is configured on the following VLANs:
  1,10,100,1000
Interface            Trusted Verify source  Rate limit(pps)
fastethernet    0/1  no      off            unlimited
fastethernet    0/2  yes     off            unlimited
     :
     :
port-channel    1    no      off            200
port-channel    2    yes     off            unlimited

>
```

(2) バインディングデータベースの確認

バインディングデータベース情報を運用コマンド show ip dhcp snooping binding で表示します。端末の MAC アドレス，IP アドレス，バインディングデータベースのエージング時間などを表示します。

運用コマンド show ip dhcp snooping binding の実行結果を次の図に示します。

図 18-16 show ip dhcp snooping binding の実行結果

```
> show ip dhcp snooping binding

Date 2008/03/04 09:32:43 UTC

Agent URL: flash
Last succeeded time: 2008/03/04 09:00:32 UTC

Total Bindings: 14
MAC Address     IP Address      Expire(min) Type     VLAN  Interface
0000.0010.1010  192.168.100.250 8           dynamic  10    fastethernet    0/7
0000.e228.15a9  192.168.200.201 58          dynamic  10    fastethernet    0/8
     :
     :

>
```

（3） DHCP snooping 統計情報の確認

DHCP snooping 統計情報を運用コマンド show ip dhcp snooping statistics で表示します。untrust ポートで受信した DHCP 総パケット数，インタフェースごとの受信した DHCP パケット数，フィルタした DHCP パケット数，受信レート制限超過で廃棄した DHCP パケット数を表示します。

運用コマンド show ip dhcp snooping statistics の実行結果を次の図に示します。

図 18-17 show ip dhcp snooping statistics の実行結果

```
> show ip dhcp snooping statistics

Date 2007/12/11 18:29:42 UTC
Database Exceeded: 0
Total DHCP Packets: 9818
Interface                       Recv      Filter   Rate over
fastethernet    0/1              796         796           0
fastethernet    0/3             1638           0        1634
fastethernet    0/4                0           0           0
     :
     :
port-channel    1                668           0           0

>
```

18.3.3 ダイナミック ARP 検査の確認

（1） ダイナミック ARP 検査統計情報の確認

ダイナミック ARP 検査の統計情報を運用コマンド show ip arp inspection statistics で表示します。中継した ARP パケット数，廃棄した ARP パケット数，廃棄 ARP パケット数の内訳を表示します。

運用コマンド show ip arp inspection statistics の実行結果を次の図に示します。

図 18-18　show ip arp inspection statistics の実行結果

```
# show ip arp inspection statistics

Date 2007/12/11 18:46:12 UTC
 Port   VLAN   Forwarded      Dropped (  Rate over  DB unmatch     Invalid )
 0/1       1          10         1511 (       1471          10          30 )
 0/3       1           0            0 (          0           0           0 )
 0/4       1         201         1463 (       1394          39          30 )
    :
    :
 ChGr1     1           0            0 (          0           0           0 )
 ChGr1    10           0            0 (          0           0           0 )

#
```

19 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。

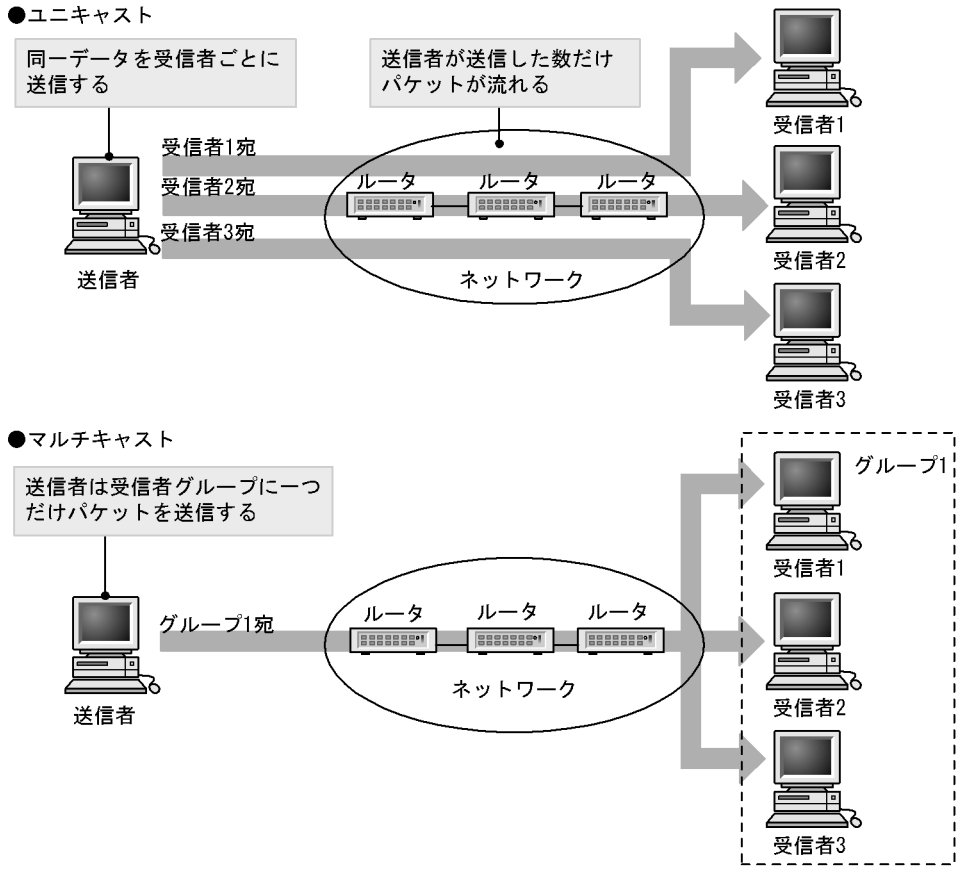
19.1　IGMP snooping/MLD snooping の概要

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。

19.1.1　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 19-1　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 19-1　マルチキャストグループアドレス

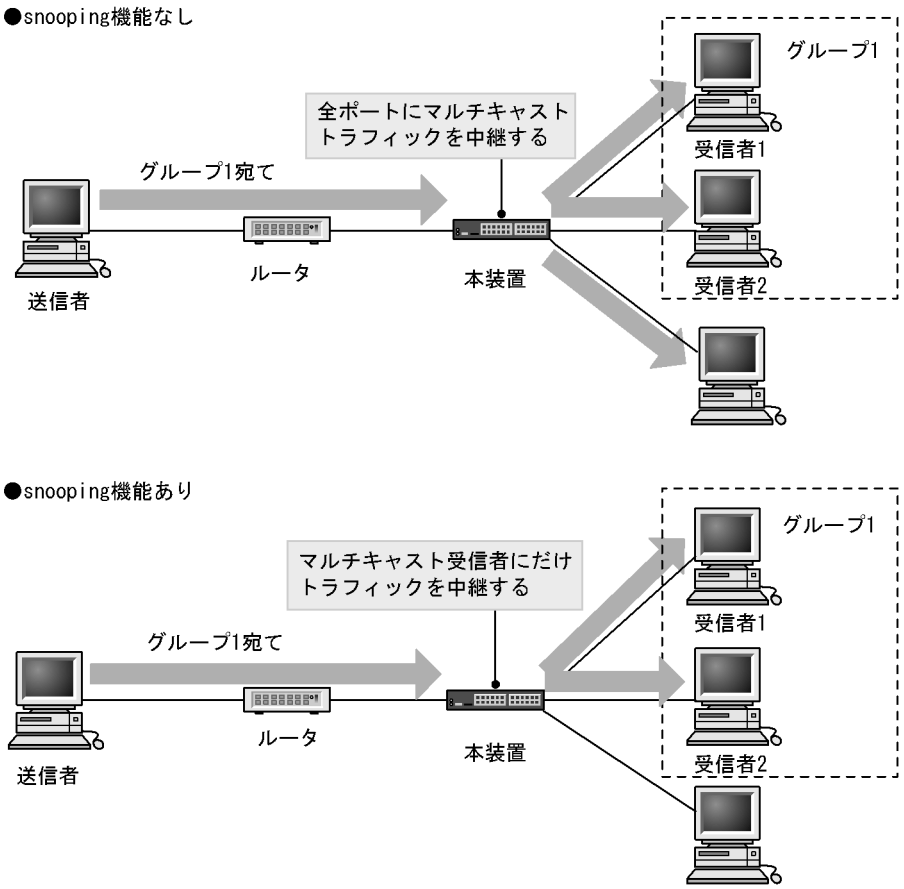
プロトコル	アドレス範囲
IPv4	224.0.0.0 ～ 239.255.255.255
IPv6	上位 8 ビットが ff(16 進数）となる IPv6 アドレス

19.1.2　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 19-2　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。

19.2 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 19-2 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	－

（凡例） －：該当なし

19.3　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。

19.3.1　MAC アドレスの学習

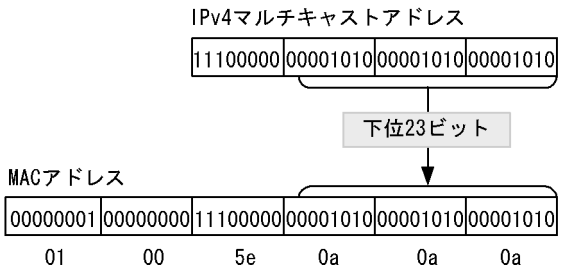
IGMP snooping が設定された VLAN で IGMP メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

（1） エントリの登録

IGMP 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，IGMP 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 19-3　IPv4 マルチキャストアドレスと MAC アドレスの対応



（2） 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。

- IGMP Leave メッセージを受信した場合
  IGMP Leave メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを１秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます)。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します)。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。
- IGMP Report 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 IGMP Report 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。

19.3.2 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 メッセージを受信したポートすべてに中継します。

「19.3.1 MAC アドレスの学習 （1）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 メッセージを受信したポートへも中継します。

19.3.3 マルチキャストルータとの接続

マルチキャストパケットの中継先にはグループ加入済みホストだけでなく隣接するマルチキャストルータも対象とします。本装置とマルチキャストルータを接続して IGMP snooping を使用する場合，マルチキャストルータへマルチキャストパケットを中継するためにマルチキャストルータと接続するポート（以降，マルチキャストルータポートとします）をコンフィグレーションで指定します。

本装置は指定したマルチキャストルータポートへは全マルチキャストパケットを中継します。

また，IGMP はルータホスト間で送受信するプロトコルであるため，IGMP メッセージはルータおよびホストが受け取ります。本装置は IGMP メッセージを次の表に示すように中継します。

表 19-3 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ている場合の中継動作です。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，IGMP Report メッセージを受信していないポートで IGMP Leave メッセージを受信した場合，クエリアの設定にかかわらず IGMP Leave メッセージは中継しません。

19.3.4 IGMP クエリア機能

IGMP クエリア機能は，VLAN 内にマルチキャストルータが存在せず，マルチキャストパケットの送信ホストと受信ホストだけが存在する環境で，本装置が IGMP Query メッセージを代理で受信ホストに対して送信する機能です。マルチキャストルータは定期的に IGMP Query メッセージを送信し，ホストからの応答を受け取ることでグループメンバーの存在有無を確認します。マルチキャストルータが存在しない場合，受信ホストからの応答がなくなるためにグループメンバーを監視することができなくなります。この機能

によって，VLAN 内にマルチキャストルータが存在しない場合でも，IGMP snooping 機能を使用可能とします。本装置では IGMP Query メッセージを 125 秒間隔で送信します。

IGMP クエリア機能を利用するためには，IGMP snooping 機能を利用する VLAN に IP アドレスを設定する必要があります。

VLAN 内に IGMP Query メッセージを送信する装置が存在する場合，IGMP Query メッセージの送信元 IP アドレスの小さい方が代表クエリアとなって IGMP Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合，本装置は IGMP クエリア機能による Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると Query メッセージの送信を開始します。本装置では代表クエリアの監視時間を 255 秒としています。

19.4　MLD snooping

ここでは，MLD snooping の機能と動作について説明します。本装置が送受信する MLD フレームのフォーマットおよび既定値は RFC2710 に従います。また，MLD バージョン 2（以降，MLDv2）メッセージのフォーマットおよび設定値は RFC3810 に従います。

19.4.1　MAC アドレスの学習

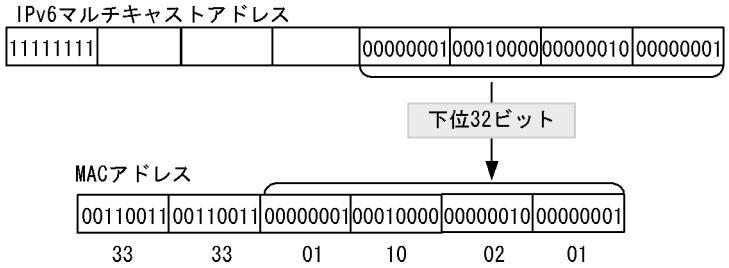
MLD snooping が設定された VLAN で MLD メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

（1） 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 19-4　IPv6 マルチキャストアドレスと MAC アドレスの対応



（2） 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（加入要求）Report メッセージを受信してから一定時間経過した場合
  マルチキャストルータは直接接続するインタフェース上にグループメンバーが存在するかを確認するために，定期的に MLD Query メッセージを送信します。本装置はルータからの MLD Query メッセージを受信した場合，VLAN 内の全ポートに中継します。MLD Query メッセージに対する応答がない場合，エントリからこのポートだけを削除します。すべてのポートから応答がない場合は，エントリ自体を削除します。
  本装置では 260 秒間 MLDv1/MLDv2 Report 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。

19.4.2　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 メッセージを受信したポートすべてに中継します。

19.4.3　マルチキャストルータとの接続

マルチキャストパケットの中継先にはグループ加入済みホストだけでなく隣接するマルチキャストルータも対象とします。本装置とマルチキャストルータを接続して MLD snooping を使用する場合，マルチキャストルータへマルチキャストパケットを中継するためにマルチキャストルータと接続するポート（以降，マルチキャストルータポートとします）をコンフィグレーションで指定します。

本装置は指定したマルチキャストルータポートへは全マルチキャストパケットを中継します。

また，MLD はルータホスト間で送受信するプロトコルであるため，MLD メッセージはルータおよびホストが受け取ります。本装置では MLD メッセージを次の表に示すように中継します。

表 19-4　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ている場合の中継動作です。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，MLDv1/MLDv2 Report（加入要求）メッセージを受信していないポートで MLDv1 Done メッセージを受信した場合，クエリアの設定にかかわらず MLDv1 Done メッセージは中継しません。

表 19-5 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ている場合の中継動作です。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，MLDv1/MLDv2（加入要求）Report 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。

19.4.4 MLD クエリア機能

MLD クエリア機能とは，VLAN 内にマルチキャストルータが存在せず，マルチキャストパケットの送信ホストと受信ホストだけが存在する環境で，本装置が MLD Query メッセージを代理で受信ホストに対して送信する機能です。マルチキャストルータは定期的に MLD Query メッセージを送信し，ホストからの応答を受け取ることでグループメンバーの存在有無を確認します。マルチキャストルータが存在しない場合，受信ホストからの応答がなくなるためにグループメンバーを監視することができなくなります。この機能によって，VLAN 内にマルチキャストルータが存在しない場合でも，MLD snooping 機能を使用可能とします。本装置では Query メッセージを 125 秒間隔で送信します。

MLD クエリア機能を利用するためには，MLD snooping 機能を利用する VLAN に 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。

19.5　IGMP snooping/MLD snooping 使用時の注意事項

（1） 運用前のシステムファンクションリソース設定について

本機能は共用のシステムファンクションリソースを使用するため，他機能との同時動作には，システムファンクションリソースの設定が必要となります。システムファンクションリソース設定については，「9.1.6　システムファンクションリソース配分の設定」を参照し，IGMP/MLD snooping 機能以外の適切な機能も合わせて選択してください。

（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 19-6　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

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。

20 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。

20.1　IGMP snooping のコンフィグレーション

20.1.1　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 20-1　コンフィグレーションコマンド一覧

コマンド名	説明
ip igmp snooping	IGMP snooping 機能を使用することを設定します。
ip igmp snooping mrouter interface	IGMP マルチキャストルータポートを設定します。
ip igmp snooping querier	IGMP クエリア機能を設定します。
no ip igmp snooping	IGMP snooping 機能の抑止を設定します。

20.1.2　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。

20.1.3　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。

20.1.4 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。

20.2 IGMP snooping のオペレーション

20.2.1 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 20-2 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 の統計情報をクリアします。

20.2.2 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 20-1 IGMP snooping の設定状態表示

```
> show igmp-snooping

Date 2006/12/15 11:10:00 UTC
VLAN counts: 1
VLAN 3253:
  IP Address:                       Querier: enable
  IGMP querying system:
  Port (4): 0/13-16
  Mrouter-port: 0/13-16
  Group counts: 253

>
```

(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 20-2 show igmp-snooping group の実行結果

```
> show igmp-snooping group

Date 2006/12/15 10:59:39 UTC
Total Groups: 500
VLAN counts: 3
VLAN 3253 Group counts: 2
  Group Address     MAC Address
   230.1.1.253       0100.5e01.01fd
     Port-list: 0/14
   230.1.1.252       0100.5e01.01fc
     Port-list: 0/14

>
```

● 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 20-3 show igmp-snooping port の実行結果

```
> show igmp-snooping port 0/13-14

Date 2006/12/15 11:00:26 UTC
Port 0/13  VLAN counts: 1
  VLAN 3253 Group counts: 0
Port 0/14  VLAN counts: 1
  VLAN 3253 Group counts: 2
    Group Address     Last Reporter      Uptime     Expires
     230.1.1.253       192.1.0.254        12:42      04:11
     230.1.1.252       192.1.0.254        12:42      04:11

>
```

20.3 MLD snooping のコンフィグレーション

20.3.1 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 20-3 コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 mld snooping	MLD snooping 機能を使用することを設定します。
ipv6 mld snooping mrouter interface	MLD マルチキャストルータポートを設定します。
ipv6 mld snooping querier	MLD クエリア機能を設定します。
no ipv6 mld snooping	MLD snooping 機能の抑止を設定します。
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。

20.3.2 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。

20.3.3 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。

20.3.4 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。

20.3.5 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。

20.4 MLD snooping のオペレーション

20.4.1 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 20-4 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 の統計情報をクリアします。

20.4.2 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 20-4 MLD snooping の設定状態表示

```
> show mld-snooping

Date 2006/12/15 14:52:18 UTC
VLAN counts: 1
VLAN 3001:
  IP Address:   Querier: enable
  MLD querying system:
  Querier version: v1
  Port (1): 0/22
  Mrouter-port:
  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 20-5 show mld-snooping group の実行結果

```
> show mld-snooping group

Date 2006/12/15 14:52:40 UTC
Total Groups: 20
VLAN counts: 20
VLAN 3001 Group counts: 1
  Group Address                              MAC Address      Version   Mode
   ff55:5555:6666:6666:7777:7777:8888:8888  3333.8888.8888   v1        -
     Port-list: 0/22
>
```

● ポートごとの参加グループ表示例を運用コマンド show mld-snooping port で確認してください。

図 20-6 show mld-snooping port の実行結果

```
> show mld-snooping port 0/22

Date 2006/12/15 14:53:07 UTC
Port 0/22  VLAN counts: 20
  VLAN 3001 Group counts: 1
    Group Address              Last Reporter              Uptime    Expires
   ff55:5555:6666:6666:7777:7777:8888:8888 fe80:0:0:0:200:1ff:fe00:200 10:35
04:20
  VLAN 3002 Group counts: 1
    Group Address              Last Reporter              Uptime    Expires
   ff55:5555:6666:6666:7777:7777:8888:8888 fe80:0:0:0:200:1ff:fe00:200 07:00
04:20

>
```

21 IPv4 インタフェース

この章では，IPv4 インタフェースの解説と操作方法について説明します。

21.1 解説

本装置は管理用として SNMP，Telnet，FTP 通信などを行うために，VLAN に IPv4 アドレスを設定することができます。本インタフェースは管理用であるため，IPv4 中継に使用できないので，ルーティングプロトコルは未サポートです。ほかのサブネットに通信するには，スタティック経路を設定して，通信を行う必要があります。

21.2　コンフィグレーション

21.2.1　コンフィグレーションコマンド一覧

IPv4 インタフェースのコンフィグレーションコマンド一覧を次の表に示します。

表 21-1　コンフィグレーションコマンド一覧

コマンド名	説明
ip address	インタフェースの IPv4 アドレスを指定します。
ip route	IPv4 のスタティック経路を指定します。

21.2.2　インタフェースの設定

［設定のポイント］

VLAN に IPv4 アドレスを設定します。IPv4 アドレスを設定するには，インタフェースコンフィグモードに移行する必要があります。

［コマンドによる設定］

1. **(config)# interface vlan 100**

   VLAN ID 100 のインタフェースコンフィグモードに移行します。

2. **(config-if)# ip address 192.168.1.1 255.255.255.0**
   (config-if)# exit

   VLAN ID 100 に IPv4 アドレス 192.168.1.1，サブネットマスク 255.255.255.0 を設定します。

21.2.3　スタティック経路の設定

［設定のポイント］

本装置はルーティングプロトコル設定をサポートしません。VLAN の外部にあるサブネットと通信するには，スタティック経路を設定する必要があります。

［コマンドによる設定］

1. **(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.254**

   宛先サブネット 192.168.2.0/24 の中継経路を 192.168.1.254 に指定します。

21.3 オペレーション

21.3.1 運用コマンド一覧

IPv4 インタフェースの運用コマンド一覧を次の表に示します。

表 21-2 運用コマンド一覧

コマンド名	説明
show ip interface	IPv4 インタフェースの状態を表示します。
show ip arp	ARP エントリ情報を表示します。
show ip route	ルートテーブルを表示します。
ping	エコーテストを行います。
traceroute	経由ルートを表示します。

21.3.2 IPv4 インタフェースの up/down 確認

IPv4 ネットワークに接続する本装置の回線や回線内のポートに IPv4 アドレスを設定したあとに，運用コマンド show ip interface を実行し，IPv4 インタフェースの up/down 状態が「Up」であることを確認してください。

図 21-1 「IPv4 インタフェース状態」の表示例

```
>show ip interface summary

Date 2006/12/12 06:16:18 UTC
VLAN3001: Up   200.1.4.1/16
VLAN3002: Up   200.2.4.1/16
VLAN3003: Up   200.3.4.1/16

>
```

21.3.3 宛先アドレスとの通信可否の確認

IPv4 ネットワークに接続している本装置のインタフェースについて，通信相手となる装置に対して通信できるかどうかを，運用コマンド ping を実行して確認してください。

図 21-2 ping の実行結果（通信可の場合）

```
> ping 192.168.0.1
Pinging 19.168.0.1 with 46 bytes of data
Reply from 192.168.0.1: count=1, bytes=46
Reply from 192.168.0.1: count=2, bytes=46
Reply from 192.168.0.1: count=3, bytes=46
Reply from 192.168.0.1: count=4, bytes=46

--- 192.168.0.1 PING Statistics ---
  Packets: sent 4, received 4, lost 0 (0% loss)
>
```

図 21-3 ping の実行結果（通信不可の場合）

```
> ping 192.168.0.1
Pinging 192.168.0.1 with 46 bytes of data
Request Timeout
Request Timeout
Request Timeout
Request Timeout

--- 192.168.0.1 Ping Statistics ---
  Packets: sent 4, received 0, lost 4 (100.% loss)
>
```

21.3.4 宛先アドレスまでの経路確認

運用コマンド traceroute を実行して，IPv4 ネットワークに接続している本装置のインタフェースから通信相手となる装置までの中継装置を確認してください。

図 21-4 traceroute の実行結果

```
> traceroute -m 3 192.168.0.1
traceroute to 192.168.0.1 over a maximum 3 hops.
  1  <10 ms    20 ms    10 ms  x.x.x.x
  2  <10 ms    10 ms   <10 ms  x.x.x.x
  3  x.x.x.x  reports: Destination host unreachable.
>
```

21.3.5 ARP 情報の確認

IPv4 ネットワークに接続する本装置の回線や回線内のポートに IPv4 アドレスを設定したあとに，運用コマンド show ip arp を実行し，本装置と隣接装置間のアドレス解決をしているか（ARP エントリ情報があるか）どうかを確認してください。

図 21-5 show ip arp の実行結果

```
> show ip arp

Date 2006/12/13 01:06:27 UTC
Total: 3
IP Address      Linklayer Address  Interface  Expire     Type
 192.0.0.1      0012.e240.0a00     VLAN0100   19min      arpa
 192.0.0.2      0012.e240.0a01     VLAN0100   17min      arpa
 192.0.0.3      0012.e240.0a02     VLAN0100   10min      arpa

>
```

21.3.6 ルートテーブルの確認

IPv4 のルートテーブルを表示します。運用コマンド show ip route で，本装置と別サブネットの装置間のルート情報が設定されているかどうかを確認してください。

図 21-6 show ip route の実行結果

```
> show ip route

Date 2006/12/13 22:54:09 UTC
Total: 4
Destination         Nexthop           Interface    Protocol
0.0.0.0/0           192.168.10.254    VLAN0001     Static
192.168.10.0/24     192.168.10.41     VLAN0001     Connected
200.1.0.0/16        200.1.4.1         VLAN3001     Connected
200.2.0.0/16        200.2.4.1         VLAN3002     Connected
>
```

付録

付録 A　準拠規格

付録 A　準拠規格

付録 A.1　RADIUS

表 A-1　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.2　NTP

表 A-2　NTP の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC2030(1996 年 10 月)	Simple Network Time Protocol (SNTP) Version4 for IPv4, IPv6 and OSI

付録 A.3　イーサネット

表 A-3　イーサネットインタフェースの準拠規格

種別	規格	名称
10BASE-T, 100BASE-TX, 1000BASE-T, 1000BASE-X	IEEE802.3x-1997	IEEE Standards for Local and Metropolitan Area Networks:Specification for 802.3 Full Duplex Operation
	IEEE802.2 1998 Edition	IEEE Standard for Information Technology - Telecommunications 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	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.4　リンクアグリゲーション

表 A-4　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.5　VLAN

表 A-5　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.6　スパニングツリー

表 A-6　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.7　IGMP snooping/MLD snooping

表 A-7　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.8　IPv4 インタフェース

表 A-8　IP バージョン 4 の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC791(1981 年 9 月)	Internet Protocol
RFC792(1981 年 9 月)	Internet Control Message Protocol
RFC826(1982 年 11 月)	An Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware
RFC922(1984 年 10 月)	Broadcasting Internet datagrams in the presence of subnets
RFC950(1985 年 8 月)	Internet Standard Subnetting Procedure
RFC1027(1987 年 10 月)	Using ARP to implement transparent subnet gateways
RFC1122(1989 年 10 月)	Requirements for Internet hosts-communication layers

索引

数字

A

D

I

L

M

P

R

S

T

V

い

う

お

こ

さ

し

す

せ

そ

た

て

に

は

ふ

ほ

ま

め

り

れ

ろ