AX2400S 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.2

Ver. 11.5 対応

AX24S-S002-D0

Alaxala

■対象製品

このマニュアルは AX2400S モデルを対象に記載しています。また，AX2400S のソフトウェア Ver. 11.5 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-L2 およびオプションライセンスによってサポートする機能について記載します。

■輸出時の注意

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

■商標一覧

Cisco は，米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。
Ethernet は，富士ゼロックス株式会社の登録商標です。
Internet Explorer は，米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。
IPX は，Novell,Inc. の商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Octpower は，日本電気（株）の登録商標です。
RSA，RSA SecurID は，RSA Security Inc. の米国およびその他の国における商標または登録商標です。
sFlow は，米国およびその他の国における米国 InMon Corp. の登録商標です。
UNIX は，The Open Group の米国ならびに他の国における登録商標です。
VitalQIP，VitalQIP Registration Manager は，Lucent technologies の商標です。
VLANaccessClient は，NEC ソフトの商標です。
VLANaccessController，VLANaccessAgent は，NEC の商標です。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
イーサネットは，富士ゼロックス株式会社の登録商標です。
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

２０１１年　 1月 （第１４版） ＡＸ ２４ Ｓ － Ｓ ００２－ Ｄ ０

■著作権

変更履歴

【Ver. 11.5 対応版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
3.10.3　IP マルチキャストパケットフロー制御補助モード	• 本項を追加しました。
13.2.10　syslog サーバへの出力	• 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. 11.4 対応版】

表　変更履歴

項目	追加・変更内容
受信側フロー検出モード	• 受信側フロー検出モード layer2-dhcp-1 の記述を追加しました。
フロー検出条件	• 受信側フロー検出モード layer2-dhcp-1 の記述を追加しました。
受信側フロー検出モード	• 受信側フロー検出モード layer2-dhcp-1 の記述を追加しました。
フロー検出条件	• 受信側フロー検出モード layer2-dhcp-1 の記述を追加しました。
認証前端末の通信許可	• DHCP snooping 関連の記述を追加しました。
概要	• DHCP snooping 関連の記述を追加しました。
DHCP snooping	• 本章を追加しました。
アップリンク・リダンダント	• 自動切り戻し機能および MAC アドレスアップデート機能サポートに伴い記述を追加しました。

【Ver. 11.2 対応版】

表　変更履歴

項目	追加・変更内容
レイヤ 2 認証と他機能との共存	• アップリンク・リダンダントの記述を追加しました。
アップリンク・リダンダント	• 本章を追加しました。

【Ver. 11.1 対応版】

表　変更履歴

項目	追加・変更内容
MAC VLAN の動的 VLAN 設定とレイヤ 2 認証	• レイヤ 2 認証機能によって MAC ポートに動的に VLAN が設定できる記述を追加しました。
認証前端末の通信許可	• 各レイヤ 2 認証単独で認証専用 IPv4 アクセスリストと ARP パケットリレー機能を設定できるようにしました。
認証済み端末のポート間移動	• Web 認証（固定 VLAN モード），MAC 認証（固定 VLAN モード）での同一 VLAN 間移動時の動作を変更しました。
RADIUS サーバ通信の dead interval 機能	• 最初の RADIUS サーバに戻す方法を変更しました。
サポート機能	•「(5) syslog サーバへの動作ログ記録」を追加しました。
端末検出動作切り替えオプション	•「(4) auto」を追加しました。

項目	追加・変更内容
RADIUS サーバ接続機能	•「(3) ポート単位認証の端末認証モード，および VLAN 単位認証（静的）で認証端末にフィルタを適用するときの設定」を追加しました。
認証処理に関する設定	•「(8) syslog サーバへの出力設定」を追加しました。
ワンタイムパスワード認証	• 本項を追加しました。
認証手順	•「(6) ワンタイムパスワード認証の Reply-Message 表示画面表示」を追加しました。
RADIUS サーバの準備	•「(1) RADIUS サーバの設定」の認証後 VLAN に関する記述を変更しました。 •「(2) Web 認証が使用する RADIUS 属性」の説明を変更しました。
認証エラーメッセージ	• 認証エラーメッセージのエラー発生理由の記述を変更しました。
Web 認証画面の情報表示	• Web 認証画面の情報表示を変更しました。
dead interval 機能による RADIUS サーバアクセスを 1 台目の RADIUS サーバに戻す	• 本項を追加しました。
Web 認証画面作成手引き	• Reply-Message 表示画面の記述を追加しました。
Reply-Message 表示画面（loginProcess.html）	• 本項を追加しました。
RADIUS サーバの準備	•「(3) 認証後 VLAN の設定」を追加しました。 •「(4) MAC 認証機能が使用する RADIUS サーバの属性」の説明を変更しました。
dead interval 機能による RADIUS サーバアクセスを 1 台目の RADIUS サーバに戻す	• 本項を追加しました。
CFM	• 本章を追加しました。

【Ver. 11.0 対応版】

表　変更履歴

項目	追加・変更内容
GSRP の解説	• GSRP VLAN グループ限定制御機能の記述を追加しました。
GSRP VLAN グループ限定制御機能	• 本項を追加しました。
GSRP の設定と運用	• GSRP VLAN グループ限定制御機能の記述を追加しました。
GSRP VLAN グループ限定制御機能の設定	• 本項を追加しました。

【Ver. 10.8 対応版】

表　変更履歴

項目	追加・変更内容
フロー検出条件	• IPv4-ICMP ヘッダのフロー検出条件に関する記述を追加しました。
フロー検出条件	• IPv4-ICMP ヘッダのフロー検出条件に関する記述を追加しました。
レイヤ 2 認証	• 本章を追加しました。
IEEE802.1X の解説	• 強制認証，認証数制限の記述を追加しました。
Web 認証の解説	• 強制認証，認証数制限，RADIUS の dead interval 機能の記述を追加しました。
Web 認証の設定と運用	• 強制認証，認証数制限，RADIUS の dead interval 機能追加に伴い記述を変更しました。

項目	追加・変更内容
MAC 認証の解説	• 強制認証，認証数制限，RADIUS の dead interval 機能の記述を追加しました。
MAC 認証の設定と運用	• 強制認証，認証数制限，RADIUS の dead interval 機能追加に伴い記述を変更しました。
装置障害時の動作	•「(2) 自動での切り替え（ダイレクトリンク障害検出による切り替え)」にダイレクト障害検出機能，GSRP スイッチ単独起動時のマスタ遷移機能の記述を追加しました。

【Ver. 10.7 対応版】

表　変更履歴

項目	追加・変更内容
Web 認証	• 従来のダイナミック VLAN モードをレガシーモードに名称を変更しました。 • 新たにダイナミック VLAN モードの記述を追加しました。 • ダイナミック VLAN モードでの URL リダイレクト機能の記述を追加しました。 • 認証除外の設定方法の記述を追加しました。
RADIUS 認証方式の事前準備	• NAS-IPv6-Address を追加しました。
MAC 認証	• ダイナミック VLAN モードの記述を追加しました。 • 認証除外の設定方法の記述を追加しました。
RADIUS 認証方式の事前準備	• NAS-IPv6-Address を追加しました。
L2 ループ検知	• 本章を追加しました。

【Ver. 10.6 対応版】

表　変更履歴

項目	追加・変更内容
Web 認証	• 固定 VLAN モードについて記述を追加しました。
MAC 認証	• 本章を追加しました。

【Ver. 10.5 対応版】

表　変更履歴

項目	追加・変更内容
フロー検出モード	• フロー検出モードの選択について記述を追記しました。 • フロー検出モード layer2-5，layer2-6 の記述を追加しました。
フロー検出条件	• TCP/UDP ポート番号の範囲指定について記述を追加しました。 • ユーザ優先度のフロー検出条件に関する記述を修正しました。
アクセスリスト	• layer2-5，layer2-6 の記述を追加しました。
IP ヘッダ・TCP/UDP ヘッダで中継・廃棄をする設定	•「(3) TCP/UDP ポート番号の範囲をフロー検出条件とする設定」を追加しました。
ユーザ優先度マッピング	•「表 2-2 ユーザ優先度と CoS 値のマッピング」に注※を追加しました。
フロー検出モード	• フロー検出モードの選択について記述を追加しました。 • フロー検出モード layer2-5，layer2-6 の記述を追加しました。
フロー検出条件	• TCP/UDP ポート番号の範囲指定について記述を追加しました。 • ユーザ優先度のフロー検出条件に関する記述を修正しました。

項目	追加・変更内容
QoS フローリスト	• フロー検出モード layer2-5，layer2-6 の記述を追加しました。
TCP/UDP ポート番号の範囲で QoS 制御する設定	• 本項を追加しました。
ユーザ優先度書き換え	• ユーザ優先度書き換えの記述を修正しました。 • ユーザ優先度引き継ぎ対応に伴う修正をしました。
ユーザ優先度引き継ぎ	• 本項を追加しました。
ユーザ優先度引き継ぎの設定	• 本項を追加しました。
ユーザ優先度引き継ぎの確認	• 本項を追加しました。
CoS 値・キューイング優先度	• ユーザ優先度引き継ぎ対応に伴う修正をしました。
ポート帯域制御	• ポート帯域制御のバーストサイズ設定について記述を追加しました。
認証手順	• ログイン画面などについて説明を追加しました。
認証エラーメッセージ	• エラーメッセージを追加しました。
Web 認証画面入れ替え機能	• 本項を追加しました。
ローカル認証方式＋内蔵 DHCP サーバ使用時の構成	• 本項を追加しました。
RADIUS 認証方式 + 内蔵 DHCP サーバ使用時の構成	• 本項を追加しました。
RADIUS 認証方式 + 外部 DHCP サーバ + 複数の認証後 VLAN 使用時の構成	• 本項を追加しました。
Web 認証画面の登録	• 本項を追加しました。
登録した Web 認証画面の削除	• 本項を追加しました。
Web 認証画面の情報表示	• 本項を追加しました。
Web 認証画面作成手引き	• 本節を追加しました。
認証 VLAN の基本的な設定	•「(1) デフォルト経路の設定」を追加しました。

【Ver. 10.4 対応版】

表　変更履歴

項目	追加・変更内容
認証 VLAN	• スイッチ間非同期モードの記述を追加しました。
GSRP の切り替え制御	• GSRP Flush request フレームの中継機能に関する記述を追加しました。
GSRP 使用時の注意事項	• GSRP Flush request フレームの中継について記述を追加しました。
sFlow 統計（フロー統計）機能	• 本章を追加しました。
ポートミラーリングの設定	• 複数モニターポートのミラーリングの記述を追加しました。

【Ver. 10.3 対応版】

表　変更履歴

項目	追加・変更内容
Web 認証	• 本章を追加しました
認証 VLAN	• 本章を追加しました
IEEE802.3ah/UDLD	• 本章を追加しました

【Ver. 10.2 対応版】

表　変更履歴

項目	追加・変更内容
フロー検出条件	• ユーザ優先度のフロー検出条件の記述を追加しました。
フィルタ使用時の注意事項	• VLAN-Tag 付きフレームに対するフィルタの注意事項を追加しました。
フロー検出条件	• ユーザ優先度のフロー検出条件の記述を追加しました。
フロー検出使用時の注意事項	• VLAN-Tag 付きフレームに対する QoS フロー検出の注意事項を追加しました。
IEEE 802.1X と他機能の共存について	•「表 5-9 IEEE 802.1X 機能とポート・VLAN 種別の共存仕様」にトンネリングポートの記述を追加しました。
ストームコントロール	• 受信したフレーム数が閾値を超えた場合にポート閉塞，トラップ送信，ログメッセージ出力を行う機能を追加しました。
SNMP を使用したネットワーク管理	• SNMPv3 の記述を追加しました。

はじめに

■対象製品およびソフトウェアバージョン

このマニュアルは AX2400S モデルを対象に記載しています。また，AX2400S のソフトウェア Ver. 11.5 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-L2 およびオプションライセンスによってサポートする機能について記載します。
操作を行う前にこのマニュアルをよく読み，書かれている指示や注意を十分に理解してください。また，このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。
なお，このマニュアルでは特に断らないかぎり OS-L2 の機能について記載しますが，オプションライセンスの機能については以下のマークで示します。

【OP-OTP】：
　オプションライセンス OP-OTP についての記述です。

【OP-VAA】：
　オプションライセンス OP-VAA についての記述です。

■このマニュアルの訂正について

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

■対象読者

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

- ネットワークシステム管理の基礎的な知識

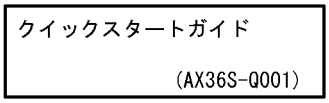
■このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しております。
http://www.alaxala.com

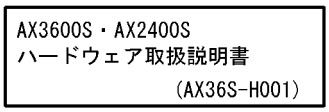
■マニュアルの読書手順

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。

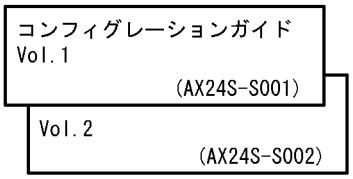
●装置の開梱から，初期導入時の基本的な設定を知りたい



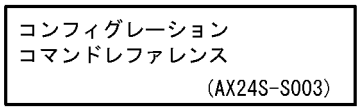
●ハードウェアの設備条件，取扱方法を調べる



●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



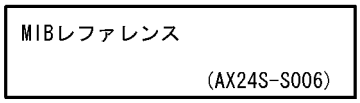
●コンフィグレーションコマンドの
入力シンタックス，パラメータ詳細
について知りたい



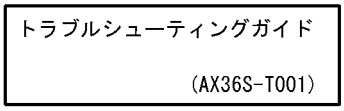
●運用コマンドの入力シンタックス，
パラメータ詳細について知りたい

●メッセージとログについて調べる

●MIBについて調べる



●トラブル発生時の対処方法について
知りたい



■このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second　　*bpsと表記する場合もあります。
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CC	Continuity Check
CDP	Cisco Discovery Protocol

CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol

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

```
            Instance
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　フィルタ

第 2 編　QoS

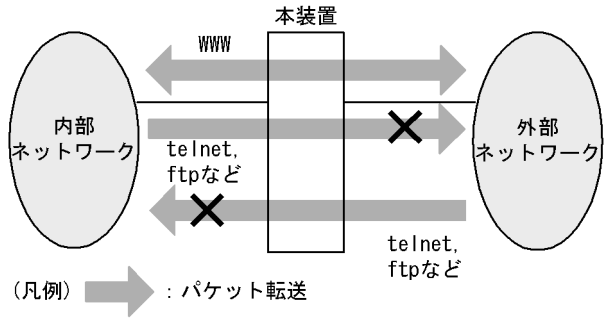
1 フィルタ

フィルタは，受信したフレームを中継したり，廃棄したりする機能です。この章ではフィルタ機能の解説と操作方法について説明します。

1.1 解説

フィルタは，受信したある特定のフレームを中継または廃棄する機能です。フィルタはネットワークのセキュリティを確保するために使用します。フィルタを使用すれば，ユーザごとにネットワークへのアクセスを制限できます。例えば，内部ネットワークと外部ネットワーク間で WWW は中継しても，telnet や ftp は廃棄したいなどの運用ができます。外部ネットワークからの不正なアクセスを防ぎ，また，内部ネットワークから外部ネットワークへ不要な情報の漏洩を防ぐことができます。フィルタを使用したネットワーク構成例を次に示します。

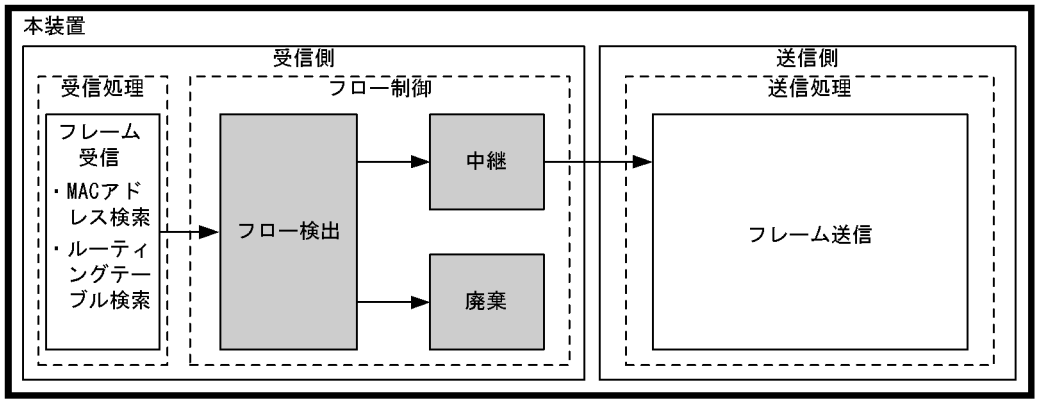
図 1-1 フィルタを使用したネットワーク構成例



1.1.1 フィルタの概要

本装置のフィルタの機能ブロックを次の図に示します。

図 1-2 本装置のフィルタの機能ブロック



この図に示したフィルタの各機能ブロックの概要を次の表に示します。

表 1-1 フィルタの各機能ブロックの概要

機能部位		機能概要
フロー制御部	フロー検出	MAC アドレスやプロトコル種別，IP アドレス，TCP/UDP のポート番号，ICMP ヘッダなどの条件に一致するフロー（特定フレーム）を検出します。
	中継・廃棄	フロー検出したフレームに対し，中継または廃棄します。

本装置では，MAC アドレス，プロトコル種別，IP アドレス，TCP/UDP のポート番号，ICMP ヘッダなどのフロー検出と，中継や廃棄という動作を組み合わせたフィルタエントリを作成し，フィルタを実施します。

本装置のフィルタの仕組みを次に示します。

1. 各インタフェースに設定したフィルタエントリをユーザが設定した優先順に検索します。
2. 一致したフィルタエントリが見つかった時点で検索を終了します。
3. 該当したフレームはフィルタエントリで設定した動作に従って，中継や廃棄が実行されます。
4. すべてのフィルタエントリに一致しなかった場合，そのフレームを廃棄します。廃棄動作の詳細は，「1.1.6　暗黙の廃棄」を参照してください。

1.1.2　フロー検出

フロー検出とは，フレームの一連の流れであるフローを MAC ヘッダ，IP ヘッダ，TCP ヘッダ，ICMP ヘッダなどの条件に基づいて検出する機能です。アクセスリストで設定します。アクセスリストの詳細は，「1.1.5　アクセスリスト」を参照してください。

本装置では，受信側イーサネットインタフェース・VLAN インタフェースで，イーサネット V2 形式および IEEE802.3 の SNAP/RFC1042 形式フレームのフロー検出ができます。設定可能なインタフェースは，受信側フロー検出モードによって変わります。なお，本装置宛ての受信フレームもフロー検出対象です。

1.1.3　受信側フロー検出モード

本装置では，ネットワーク構成や運用形態を想定して次の表に示す受信側フロー検出モードを用意しています。使い方に合わせて選択してください。また，受信側フロー検出モードを選択する際の目安について次に示します。MAC 条件，IPv4 条件，および IPv6 条件の詳細は「1.1.4　フロー検出条件」を参照してください。

- MAC 条件でフレームを検出したい場合は，layer2-1 を使用してください。
- IPv4 条件に特化してフレームを検出したい場合は，layer2-2，layer2-5，および layer2-6 のどれかを使用してください。TCP/UDP ポート番号の範囲指定は layer2-5 および layer2-6 で指定可能です。
- IPv4 条件および IPv6 条件でフレームを検出したい場合は，layer2-3，layer2-4 のどちらかを使用してください。
- IPv4 条件でフレームを検出して，かつ DHCP snooping の端末フィルタを使用したい場合は，layer2-dhcp-1 を使用してください。

受信側フロー検出モードは flow detection mode コマンドで指定します。なお，選択した受信側フロー検出モードはフィルタ・QoS で共通です。

受信側フロー検出モードを指定しない場合，layer2-2 がデフォルトのモードとして設定されます。

受信側フロー検出モードとフロー動作の関係を次の表に示します。

表 1-2　受信側フロー検出モードとフロー動作の関係

受信側フロー検出モード名称	運用目的	フロー動作	検出対象インタフェース
layer2-1	IP パケットやそれ以外のフレームのフロー制御を行いたい場合に使用します。	MAC アドレス，イーサネットタイプなどの MAC ヘッダでフレームを検出します。	イーサネット，VLAN

受信側フロー検出モード名称	運用目的	フロー動作	検出対象インタフェース
layer2-2	IPv4 パケットに特化し，きめ細かいフロー制御を行いたい場合に使用します。	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。	イーサネット，VLAN
layer2-3	IPv4，IPv6 パケットに特化したフロー制御を行いたい場合に使用します。	IPv4 パケットは，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。IPv6 パケットは，送信元 IP アドレスでフレームを検出します。	イーサネット
layer2-4	IPv4，IPv6 パケットに特化したフロー制御を行いたい場合に使用します。	IPv4 パケットは，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。IPv6 パケットは，宛先 IP アドレスでフレームを検出します。	イーサネット
layer2-5	IPv4 パケットに特化し，きめ細かいフロー制御を行いたい場合に使用します。フロー検出で TCP/UDP ポート番号の範囲指定ができます。宛先ポート番号のフロー検出を重視したモードです。	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダでフレームを検出します。	イーサネット，VLAN
layer2-6	IPv4 パケットに特化し，きめ細かいフロー制御を行いたい場合に使用します。フロー検出で TCP/UDP ポート番号の範囲指定ができます。送信元ポート番号のフロー検出を重視したモードです。	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。	イーサネット，VLAN
layer2-dhcp-1	IPv4 パケットに特化したフロー制御を行い，かつ DHCP snooping の端末フィルタを使用したい場合に使用します。	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。	イーサネット

1.1.4 フロー検出条件

フロー検出するためには，コンフィグレーションでフローを識別するための条件を指定します。受信側フロー検出モードごとの指定可能なフロー検出条件を次の表に示します。

表 1-3 指定可能なフロー検出条件（1/4）

種別		設定項目	layer2-1		layer2-2	
			イーサネット	VLAN	イーサネット	VLAN
MAC 条件	コンフィグレーション	VLAN ID ※1	○	－	－	－
	MAC ヘッダ	送信元 MAC アドレス	○	○	－	－
		宛先 MAC アドレス	○	○	－	－
		イーサネットタイプ	○	○	－	－
		ユーザ優先度※2	○	○	－	－
IPv4 条件	コンフィグレーション	VLAN ID ※1	－	－	○	－

種別		設定項目		layer2-1		layer2-2	
				イーサネット	VLAN	イーサネット	VLAN
	MAC ヘッダ	ユーザ優先度※2		－	－	○	○
	IPv4 ヘッダ※3	上位プロトコル		－	－	○	○
		送信元 IP アドレス		－	－	○	○
		宛先 IP アドレス		－	－	○	○
		ToS		－	－	○	○
		DSCP		－	－	○	○
		Precedence		－	－	○	○
	IPv4-TCP ヘッダ	送信元ポート番号	単一指定（eq）	－	－	○	○
			範囲指定（range）	－	－	－	－
		宛先ポート番号	単一指定（eq）	－	－	○	○
			範囲指定（range）	－	－	－	－
		TCP 制御フラグ※4		－	－	○	○
	IPv4-UDP ヘッダ	送信元ポート番号	単一指定（eq）	－	－	○	○
			範囲指定（range）	－	－	－	－
		宛先ポート番号	単一指定（eq）	－	－	○	○
			範囲指定（range）	－	－	－	－
	IPv4-ICMP ヘッダ	ICMP タイプ値		－	－	○	○
		ICMP コード値		－	－	○	○
IPv6 条件	コンフィグレーション	VLAN ID※1		－	－	－	－
	MAC ヘッダ	ユーザ優先度※2		－	－	－	－
	IPv6 ヘッダ	送信元 IP アドレス		－	－	－	－
		宛先 IP アドレス		－	－	－	－

表 1-4　指定可能なフロー検出条件（2/4）

種別		設定項目	layer2-3	layer2-4
			イーサネット	イーサネット
MAC 条件	コンフィグレーション	VLAN ID※1	－	－
	MAC ヘッダ	送信元 MAC アドレス	－	－
		宛先 MAC アドレス	－	－
		イーサネットタイプ	－	－

種別		設定項目		layer2-3	layer2-4
				イーサネット	イーサネット
		ユーザ優先度※2		−	−
IPv4 条件	コンフィグレーション	VLAN ID※1		○	○
	MAC ヘッダ	ユーザ優先度※2		○	○
	IPv4 ヘッダ※3	上位プロトコル		○	○
		送信元 IP アドレス		○	○
		宛先 IP アドレス		○	○
		ToS		○	○
		DSCP		○	○
		Precedence		○	○
	IPv4-TCP ヘッダ	送信元ポート番号	単一指定（eq）	○	○
			範囲指定（range）	−	−
		宛先ポート番号	単一指定（eq）	○	○
			範囲指定（range）	−	−
		TCP 制御フラグ※4		○	○
	IPv4-UDP ヘッダ	送信元ポート番号	単一指定（eq）	○	○
			範囲指定（range）	−	−
		宛先ポート番号	単一指定（eq）	○	○
			範囲指定（range）	−	−
	IPv4-ICMP ヘッダ	ICMP タイプ値		○	○
		ICMP コード値		○	○
IPv6 条件	コンフィグレーション	VLAN ID※1		○	○
	MAC ヘッダ	ユーザ優先度※2		○	○
	IPv6 ヘッダ	送信元 IP アドレス		○	−
		宛先 IP アドレス		−	○

表 1-5　指定可能なフロー検出条件（3/4）

種別		設定項目	layer2-5		layer2-6	
			イーサネット	VLAN	イーサネット	VLAN
MAC 条件	コンフィグレーション	VLAN ID※1	−	−	−	−
	MAC ヘッダ	送信元 MAC アドレス	−	−	−	−
		宛先 MAC アドレス	−	−	−	−

種別		設定項目		layer2-5		layer2-6	
				イーサネット	VLAN	**イーサネット**	VLAN
		イーサネットタイプ		―	―	―	―
		ユーザ優先度※2		―	―	―	―
IPv4 条件	コンフィグレーション	VLAN ID※1		○	―	○	―
	MAC ヘッダ	ユーザ優先度※2		○	○	○	○
	IPv4 ヘッダ※3	上位プロトコル		○	○	○	○
		送信元 IP アドレス		○	○	○	○
		宛先 IP アドレス		○	○	○	○
		ToS		○	○	○	○
		DSCP		○	○	○	○
		Precedence		○	○	○	○
	IPv4-TCP ヘッダ	送信元ポート番号	単一指定（eq）	○※5	○※5	○	○
			範囲指定（range）	○※5	○※5	○※5	○※5
		宛先ポート番号	単一指定（eq）	○	○	○※5	○※5
			範囲指定（range）	○※5	○※5	○※5	○※5
		TCP 制御フラグ※4		○	○	○	○
	IPv4-UDP ヘッダ	送信元ポート番号	単一指定（eq）	○※5	○※5	○	○
			範囲指定（range）	○※5	○※5	○※5	○※5
		宛先ポート番号	単一指定（eq）	○	○	○※5	○※5
			範囲指定（range）	○※5	○※5	○※5	○※5
	IPv4-ICMP ヘッダ	ICMP タイプ値		―	―	○	○
		ICMP コード値		―	―	○	○
IPv6 条件	コンフィグレーション	VLAN ID※1		―	―	―	―
	MAC ヘッダ	ユーザ優先度※2		―	―	―	―
	IPv6 ヘッダ	送信元 IP アドレス		―	―	―	―
		宛先 IP アドレス		―	―	―	―

表 1-6　指定可能なフロー検出条件（4/4）

種別		設定項目	layer2-dhcp-1
			イーサネット
MAC 条件	コンフィグレーション	VLAN ID※1	―

種別		設定項目		layer2-dhcp-1
				イーサネット
	MAC ヘッダ	送信元 MAC アドレス		－
		宛先 MAC アドレス		－
		イーサネットタイプ		－
		ユーザ優先度※2		－
IPv4 条件	コンフィグレーション	VLAN ID※1		○
	MAC ヘッダ	ユーザ優先度※2		○
	IPv4 ヘッダ※3	上位プロトコル		○
		送信元 IP アドレス		○
		宛先 IP アドレス		○
		ToS		○
		DSCP		○
		Precedence		○
	IPv4-TCP ヘッダ	送信元ポート番号	単一指定（eq）	○
			範囲指定（range）	－
		宛先ポート番号	単一指定（eq）	○
			範囲指定（range）	－
		TCP 制御フラグ※4		○
	IPv4-UDP ヘッダ	送信元ポート番号	単一指定（eq）	○
			範囲指定（range）	－
		宛先ポート番号	単一指定（eq）	○
			範囲指定（range）	－
	IPv4-ICMP ヘッダ	ICMP タイプ値		○
		ICMP コード値		○
IPv6 条件	コンフィグレーション	VLAN ID※1		－
	MAC ヘッダ	ユーザ優先度※2		－
	IPv6 ヘッダ	送信元 IP アドレス		－
		宛先 IP アドレス		－

（凡例）○：指定できる　　－：指定できない

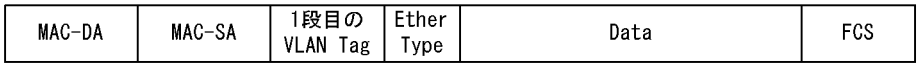
注※ 1

本装置のフロー検出で検出できる VLAN ID は，VLAN コンフィグレーションで入力した VLAN に対して付与する値です。入力フレームの属する VLAN ID を検出します。

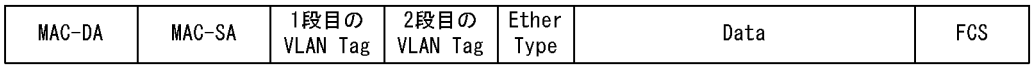
注※ 2

次に示すフレームについてはユーザ優先度を検出できません。常に，ユーザ優先度 3 として検出します。
・VLAN Tag なしのフレーム
・VLAN トンネリングを設定したポートで受信したフレーム
・Tag 変換機能により Tag 変換されたフレーム
VLAN Tag が複数あるフレームに対してユーザ優先度を検出する場合，MAC アドレス側から 1 段目の VLAN Tag にあるユーザ優先度が対象となります。次の図に VLAN Tag が複数あるフレームの例を示します。

（i）VLAN Tag 1段のフォーマット

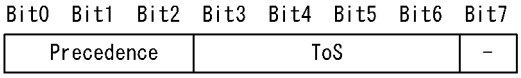


（ii）VLAN Tag 2段のフォーマット

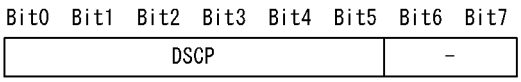


注※ 3

ToS フィールドの指定についての補足
ToS　　：ToS フィールドの 3 ビット～ 6 ビットの値です。
Precedence：ToS フィールドの上位 3 ビットの値です。



DSCP　　：ToS フィールドの上位 6 ビットの値です。



注※ 4

ack/fin/psh/rst/syn/urg フラグが 1 のパケットを検出します。

注※ 5

ハードウェアリソースである TCP/UDP ポート番号検出パターンを使用します。TCP/UDP ポート番号検出パターンの使用例については，マニュアル「コンフィグレーションガイド Vol.1　3.2.4 フィルタ・QoS」を参照してください。

1.1.5 アクセスリスト

フィルタのフロー検出を実施するためにはコンフィグレーションでアクセスリストを設定します。フロー検出条件に応じて設定するアクセスリストが異なります。また，フロー検出条件ごとに検出可能なフレーム種別が異なります。フロー検出条件と対応するアクセスリスト，および検出可能なフレーム種別の関係を次の表に示します。

表 1-7　フロー検出条件と対応するアクセスリスト，検出可能なフレーム種別の関係

フロー検出条件	対応するアクセスリスト	対応する受信側フロー検出モード	検出可能なフレーム種別		
			非 IP	IPv4	IPv6
MAC 条件	mac access-list	layer2-1	○	○	○
IPv4 条件	access-list ip access-list	layer2-2, layer2-3, layer2-4, layer2-5, layer2-6, layer2-dhcp-1	―	○	―
IPv6 条件	ipv6 access-list	layer2-3, layer2-4	―	―	○

（凡例）○：検出できる　　－：検出できない

アクセスリストのインタフェースへの適用は，アクセスグループコマンドで実施します。適用順序は，アクセスリストのパラメータであるシーケンス番号によって決定します。また，アクセスリストごとに，フィルタエントリの検索は独立して実施します。そのため，フレームが複数のフィルタエントリに一致することがあります。複数のフィルタエントリに一致した場合，実際に動作するのは単一のフィルタエントリです。

(1) イーサネットインタフェースと VLAN インタフェース同時に一致した場合の動作

イーサネットインタフェースと，該当するイーサネットインタフェースが属している VLAN インタフェースに対してフィルタエントリを設定し，該当するイーサネットインタフェースからの受信フレームに対してフィルタを実施すると，複数のフィルタエントリに一致する場合があります。この場合，廃棄動作を指定したフィルタエントリ（暗黙の廃棄のエントリを含む）が優先となります。イーサネットインタフェース，および VLAN インタフェース共に中継動作を指定したフィルタエントリに一致する場合はイーサネットインタフェース上のフィルタエントリを優先します。複数のフィルタエントリに一致した場合の動作を次の表に示します。

表 1-8　複数のフィルタエントリに一致した場合の動作

複数フィルタエントリ一致となる組み合わせ		有効になるフィルタエントリ	
イーサネット	VLAN	インタフェース	動作
中継	中継	イーサネット	中継
中継	廃棄	VLAN	廃棄
廃棄	中継	イーサネット	廃棄
廃棄	廃棄	イーサネット	廃棄

この条件に該当する受信側フロー検出モードは，layer2-1，layer2-2，layer2-5，layer2-6 です。

(2) 廃棄できないフレーム

次に示すフレームは，フィルタの有無にかかわらず，フレームを廃棄できません。

本装置が受信するフレームのうち次のフレーム

- ARP フレーム
- 回線テストに使用するフレーム
- MAC アドレス学習の移動検出とみなしたフレーム

1.1.6 暗黙の廃棄

フィルタを設定したインタフェースでは，フロー検出条件に一致しないフレームは廃棄します。

暗黙の廃棄のフィルタエントリは，アクセスリストを生成すると自動生成されます。アクセスリストを一つも設定しない場合，すべてのフレームを中継します。

1.1.7 フィルタ使用時の注意事項

(1) 複数フィルタエントリ一致時の動作

フレームが複数のフィルタエントリに一致した場合，一致したフィルタエントリの統計情報が採られます。

(2) VLAN-Tag 付きフレームに対するフィルタ

3 段以上の VLAN-Tag があるフレームに対して，MAC 条件のイーサネットタイプ，IPv4 条件，または IPv6 条件をフロー検出条件としたフィルタを実施できません。

2 段の VLAN-Tag があるフレームに対して，MAC 条件のイーサネットタイプ，IPv4 条件，または IPv6 条件をフロー検出条件としたフィルタを実施するためには，次の条件をすべて満たす必要があります。

- 本装置のどれかのポートで，VLAN トンネリング機能または Tag 変換機能が動作している
- フレームを受信したポートが，Tag 変換機能が動作していないトランクポートである

(3) IPv4 フラグメントパケットに対するフィルタ

IPv4 フラグメントパケットに対して TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件としたフィルタを行った場合，2 番目以降のフラグメントパケットは TCP/UDP ヘッダ・ICMP ヘッダがパケット内にないため，検出できません。フラグメントパケットを含めたフィルタを実施する場合は，フロー検出条件に MAC ヘッダ，IP ヘッダを指定してください。

(4) フィルタエントリ適用時の動作

本装置では，インタフェースに対してフィルタを適用する※と，暗黙の廃棄エントリから適用します。そのため，ユーザが設定したフィルタエントリが適用されるまでの間，暗黙の廃棄に一致するフレームが一時的に廃棄されます。また，暗黙の廃棄エントリの統計情報が採られます。

注※

- 1 エントリ以上を設定したアクセスリストをアクセスグループコマンドによりインタフェースに適用する場合
- アクセスリストをアクセスグループコマンドにより適用し，ひとつ目のエントリを追加する場合

(5) フィルタエントリ変更時の動作

本装置では，インタフェースに適用済みのフィルタエントリを変更すると，変更が反映されるまでの間，検出の対象となるフレームが検出されなくなります。そのため，一時的にほかのフィルタエントリまたは暗黙の廃棄エントリで検出されます。

(6) ほかの機能との同時動作

以下の場合フレームは廃棄しますが，インタフェースに対してフィルタエントリを設定し一致した場合，一致したフィルタエントリの統計情報が採られます。

- VLAN のポートのデータ転送状態が Blocking（データ転送停止中）の状態で，該当ポートからフレームを受信した場合
- プロトコル VLAN・MAC VLAN で，VLAN-Tag 付きフレームを受信した場合
- ポート間中継遮断機能で指定したポートからフレームを受信した場合
- ネイティブ VLAN をトランクポートで送受信する VLAN に設定しないで，VLAN-Tag なしフレームを受信した場合
- トランクポートで送受信する VLAN に設定していない VLAN-Tag 付きフレームを受信した場合
- アクセスポートで VLAN-Tag 付きフレームを受信した場合
- 廃棄動作を指定したフィルタエントリ（暗黙の廃棄のエントリを含む）に一致するフレームを受信した場合
- DHCP snooping の端末フィルタによってフレームが廃棄された場合
- 認証専用 IPv4 アクセスリストによってフレームが廃棄された場合

1.2 コンフィグレーション

1.2.1 コンフィグレーションコマンド一覧

フィルタで使用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 1-9 コンフィグレーションコマンド一覧

コマンド名	説明
access-list	IPv4 フィルタとして動作するアクセスリストを設定します。
deny	IPv4 フィルタでのアクセスを破棄する条件を指定します。
ip access-group	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 IPv4 フィルタを適用し，IPv4 フィルタ機能を有効にします。
ip access-list extended	IPv4 パケットフィルタとして動作するアクセスリストを設定します。
ip access-list resequence	IPv4 アドレスフィルタおよび IPv4 パケットフィルタのフィルタ条件適用順序のシーケンス番号を再設定します。
ip access-list standard	IPv4 アドレスフィルタとして動作するアクセスリストを設定します。
ipv6 access-list	IPv6 フィルタとして動作するアクセスリストを設定します。
ipv6 access-list resequence	IPv6 フィルタのフィルタ条件適用順序のシーケンス番号を再設定します。
ipv6 traffic-filter	イーサネットインタフェースに対して IPv6 フィルタを適用し，IPv6 フィルタ機能を有効にします。
mac access-group	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 MAC フィルタを適用し，MAC フィルタ機能を有効にします。
mac access-list extended	MAC フィルタとして動作するアクセスリストを設定します。
mac access-list resequence	MAC フィルタのフィルタ条件適用順序のシーケンス番号を再設定します。
permit	IPv4 フィルタでのアクセスを中継する条件を指定します。
remark	フィルタの補足説明を指定します。
flow detection mode ※	フィルタ・QoS 制御の受信側フロー検出モードを設定します。

注※

「コンフィグレーションコマンドレファレンス　22. フロー検出モード」を参照してください。

1.2.2 受信側フロー検出モードの設定

フィルタの受信側フロー検出モードを指定する例を次に示します。

[設定のポイント]

受信側フロー検出モードは，ハードウェアの基本的な動作条件を決定するため，最初に設定します。

[コマンドによる設定]

1. **(config)# flow detection mode layer2-3**

受信側フロー検出モード layer2-3 を有効にします。

1.2.3 MAC ヘッダで中継・廃棄をする設定

MAC ヘッダをフロー検出条件として，フレームを中継・廃棄指定する例を次に示します。

[設定のポイント]

フレーム受信時に MAC ヘッダによってフロー検出を行い，フィルタエントリに一致したフレームを廃棄・中継します。

[コマンドによる設定]

1. **(config)# mac access-list extended IPX_DENY**
   mac access-list（IPX_DENY）を作成します。本リストを作成することによって，MAC フィルタの動作モードに移行します。

2. **(config-ext-macl)# deny any any ipx**
   イーサネットタイプが IPX のフレームを廃棄する MAC フィルタを設定します。

3. **(config-ext-macl)# permit any any**
   すべてのフレームを中継する MAC フィルタを設定します。

4. **(config-ext-macl)# exit**
   MAC フィルタの動作モードからグローバルコンフィグレーションモードに戻ります。

5. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

6. **(config-if)# mac access-group IPX_DENY in**
   受信側に MAC フィルタを有効にします。

1.2.4 IP ヘッダ・TCP/UDP ヘッダで中継・廃棄をする設定

(1) IPv4 アドレスをフロー検出条件とする設定

IPv4 アドレスをフロー検出条件とし，フレームを中継・廃棄指定する例を次に示します。

[設定のポイント]

フレーム受信時に送信元 IPv4 アドレスによってフロー検出を行い，フィルタエントリに一致したフレームを中継します。フィルタエントリに一致しない IP パケットはすべて廃棄します。

[コマンドによる設定]

1. **(config)# ip access-list standard FLOOR_A_PERMIT**
   ip access-list（FLOOR_A_PERMIT）を作成します。本リストを作成することによって，IPv4 アドレスフィルタの動作モードに移行します。

2. **(config-std-nacl)# permit 192.168.0.0 0.0.0.255**
   送信元 IP アドレス 192.168.0.0/24　ネットワークからのフレームを中継する IPv4 アドレスフィルタを設定します。

3. **(config-ext-nacl)# exit**

IPv4 アドレスフィルタの動作モードから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 vlan 10**
   VLAN10 のインタフェースモードに移行します。

5. **(config-if)# ip access-group FLOOR_A_PERMIT in**
   受信側に IPv4 フィルタを有効にします。

(2) IPv4 パケットをフロー検出条件とする設定

IPv4 telnet パケットをフロー検出条件とし，フレームを中継・廃棄指定する例を次に示します。

[設定のポイント]

フレーム受信時に IP ヘッダ・TCP/UDP ヘッダによってフロー検出を行い，フィルタエントリに一致したフレームを廃棄します。

[コマンドによる設定]

1. **(config)# ip access-list extended TELNET_DENY**
   ip access-list（TELNET_DENY）を作成します。本リストを作成することによって，IPv4 パケットフィルタの動作モードに移行します。

2. **(config-ext-nacl)# deny tcp any any eq telnet**
   telnet のパケットを廃棄する IPv4 パケットフィルタを設定します。

3. **(config-ext-nacl)# permit ip any any**
   すべてのフレームを中継する IPv4 パケットフィルタを設定します。

4. **(config-ext-nacl)# exit**
   IPv4 アドレスフィルタの動作モードからグローバルコンフィグレーションモードに戻ります。

5. **(config)# interface vlan 10**
   VLAN10 のインタフェースモードに移行します。

6. **(config-if)# ip access-group TELNET_DENY in**
   受信側に IPv4 フィルタを有効にします。

(3) TCP/UDP ポート番号の範囲をフロー検出条件とする設定

UDP ポート番号の範囲をフロー検出条件とし，フレームを中継・廃棄指定する例を次に示します。

[設定のポイント]

フレーム受信時に UDP ヘッダの宛先ポート番号の範囲によってフロー検出を行い，フィルタエントリに一致したフレームを廃棄します。

[コマンドによる設定]

1. **(config)# ip access-list extended PORT_RANGE_DENY**
   ip access-list（PORT_RANGE_DENY）を作成します。本リストを作成することによって，IPv4 パケットフィルタの動作モードに移行します。

2. **(config-ext-nacl)# deny udp any any range 10 20**
   UDP ヘッダの宛先ポート番号が 10 ～ 20 のパケットを廃棄する IPv4 パケットフィルタを設定します。

3. **(config-ext-nacl)# permit ip any any**
   すべてのフレームを中継する IPv4 パケットフィルタを設定します。

4. **(config-ext-nacl)# exit**
   IPv4 アドレスフィルタの動作モードからグローバルコンフィグレーションモードに戻ります。

5. **(config)# interface vlan 10**
   VLAN10 のインタフェースモードに移行します。

6. **(config-if)# ip access-group PORT_RANGE_DENY in**
   受信側に IPv4 フィルタを有効にします。

(4) IPv6 パケットをフロー検出条件とする設定

IPv6 パケットをフロー検出条件として，フレームを中継・廃棄指定する例を次に示します。

[設定のポイント]

フレーム受信時に IP アドレスによってフロー検出を行い，フィルタエントリに一致したフレームを中継します。フィルタエントリに一致しない IP パケットはすべて廃棄します。

[コマンドによる設定]

1. **(config)# ipv6 access-list FLOOR_B_PERMIT**
   ipv6 access-list(FLOOR_B_PERMIT) を作成します。本リストを作成することによって，IPv6 パケットフィルタの動作モードに移行します。

2. **(config-ipv6-acl)# permit ipv6 2001:100::1/64 any**
   送信元 IP アドレス 2001:100::1/64 からのフレームを中継する IPv6 パケットフィルタを設定します。

3. **(config-ipv6-acl)# exit**
   IPv6 パケットフィルタの動作モードから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 gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

5. **(config-if)# ipv6 traffic-filter FLOOR_B_PERMIT in**
   受信側に IPv6 フィルタを有効にします。

1.2.5 複数インタフェースフィルタの設定

複数のイーサネットインタフェースにフィルタを指定する例を次に示します。

[設定のポイント]

config-if-range モードで複数のイーサネットインタフェースにフィルタを設定できます。

[コマンドによる設定]

1. **(config)# access-list 10 permit host 192.168.0.1**
   ホスト 192.168.0.1 からだけフレームを中継する IPv4 アドレスフィルタを設定します。

2. **(config)# interface range gigabitethernet 0/1-4**
   ポート 0/1-4 のインタフェースモードに移行します。

3. **(config-if-range)# ip access-group 10 in**
   受信側に IPv4 フィルタを有効にします。

1.3 オペレーション

show access-filter コマンドによって，設定した内容が反映されているかどうかを確認します。

1.3.1 運用コマンド一覧

フィルタで使用する運用コマンド一覧を次の表に示します。

表 1-10 運用コマンド一覧

コマンド名	説明
show access-filter	アクセスグループコマンド (mac access-group，ip access-group，ipv6 traffic-filter) で設定したアクセスリスト (mac access-list，access-list，ip access-list，ipv6 access-list) の統計情報を表示します。
clear access-filter	アクセスグループコマンド (mac access-group，ip access-group，ipv6 traffic-filter) で設定したアクセスリスト (mac access-list，access-list，ip access-list，ipv6 access-list) の統計情報をクリアします。

1.3.2 フィルタの確認

(1) イーサネットインタフェースに設定されたエントリの確認

イーサネットインタフェースにフィルタを設定した場合の動作確認の方法を次の図に示します。

図 1-3 イーサネットインタフェースにフィルタを設定した場合の動作確認

```
> show access-filter 0/1 IPX_DENY
Date 2005/12/01 12:00:00 UTC
Using Port:0/1 in
Extended MAC access-list: IPX_DENY
      remark "deny only ipx"
      deny any any ipx
         matched packets       :  74699826
      permit any any
         matched packets       :    264176
      implicitly denied packets:         0
```

指定したポートのフィルタに「Extended MAC access-list」が表示されることを確認します。

(2) VLAN インタフェースに設定されたエントリの確認

VLAN インタフェースにフィルタを設定した場合の動作確認の方法を次の図に示します。

図 1-4 VLAN インタフェースにフィルタを設定した場合の動作確認

```
> show access-filter interface vlan 10 FLOOR_A_PERMIT
Date 2005/12/01 12:00:00 UTC
Using Interface:vlan 10 in
Standard IP access-list: FLOOR_A_PERMIT
      remark "permit only Floor-A"
      permit 192.168.0.0 0.0.0.255 any
         matched packets       :  74699826
      implicitly denied packets:      2698
```

指定した VLAN のフィルタに「Standard IP access-list」が表示されることを確認します。

2 QoS 制御の概要

QoS 制御は，帯域監視・マーカー・優先度決定・帯域制御によって通信品質を制御し，回線の帯域やキューのバッファ容量などの限られたネットワーク資源を有効に利用するための機能です。この章では，本装置の QoS 制御について説明します。

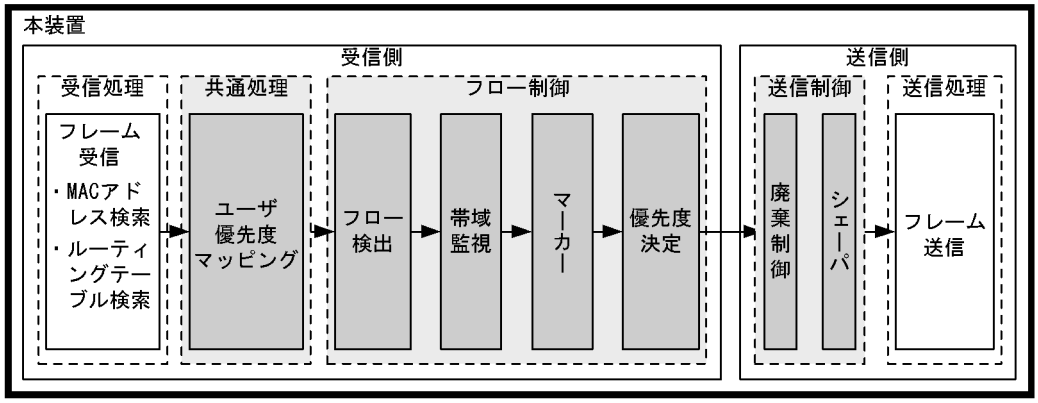
2.1 QoS 制御構造

ネットワークを利用したサービスの多様化に伴い，通信品質を保証しないベストエフォート型のトラフィックに加え，実時間型・帯域保証型のトラフィックが増加しています。本装置の QoS 制御を使用することによって，トラフィック種別に応じた通信品質を提供できます。

本装置の QoS 制御は，回線の帯域やキューのバッファ容量などの限られたネットワーク資源を有効に使用できます。アプリケーションごとに要求されるさまざまな通信品質を満たすために，QoS 制御を使用しネットワーク資源を適切に分配します。

本装置の QoS 制御の機能ブロックを次の図に示します。

図 2-1 本装置の QoS 制御の機能ブロック



（凡例）□：この節で説明するブロック

図に示した QoS 制御の各機能ブロックの概要を次の表に示します。

表 2-1 QoS 制御の各機能ブロックの概要

機能部位		機能概要
受信処理部	フレーム受信	フレームを受信し，MAC アドレステーブル検索やルーティングテーブル検索を実施します。
共通処理部	ユーザ優先度マッピング	受信フレームの VLAN Tag のユーザ優先度に従い，優先度を決定します。
フロー制御部	フロー検出	MAC ヘッダやプロトコル種別，IP アドレス，ポート番号，ICMP ヘッダなどの条件に一致するフローを検出します。
	帯域監視	フローごとに帯域を監視して，帯域を超えたフローに対してペナルティを与えます。
	マーカー	IP ヘッダ内の DSCP や VLAN Tag のユーザ優先度を書き換える機能です。
	優先度決定	フローに対する優先度や，廃棄されやすさを示すキューイング優先度を決定します。
送信制御部	廃棄制御	パケットの優先度とキューの状態に応じて，該当フレームをキューイングするか廃棄するかを制御します。
	シェーパ	各キューからのフレームの出力順序および出力帯域を制御します。
送信処理部	フレーム送信	シェーパによって制御されたフレームを送信します。

本装置の QoS 制御は，受信フレームの優先度をユーザ優先度マッピング，またはフロー制御によって決定

します。ユーザ優先度マッピングは，受信フレームの VLAN Tag 内にあるユーザ優先度に基づいて優先度を決定します。ユーザ優先度ではなく，MAC アドレスや IP アドレスなどの特定の条件に一致するフレームに対して優先度を決定したい場合は，フロー制御を使用します。

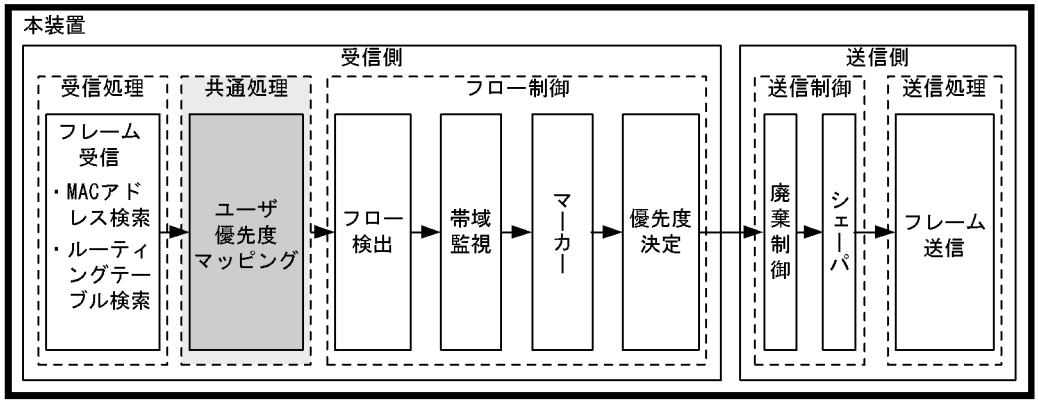
フロー制御による優先度の決定は，ユーザ優先度マッピングよりも優先されます。また，フロー制御は，優先度決定のほかに帯域監視やマーカーも実施することができます。フロー検出で検出したフローに対して，帯域監視，マーカー，優先度決定の各機能は同時に動作することができます。

送信制御は，ユーザ優先度マッピングやフロー制御によって決定した優先度に基づいて，廃棄制御やシェーパを実施します。

2.2 共通処理解説

この節で説明するユーザ優先度マッピングの位置づけを次の図に示します。

図 2-2 ユーザ優先度マッピングの位置づけ



（凡例）：この節で説明するブロック

2.2.1 ユーザ優先度マッピング

ユーザ優先度マッピングは，受信フレームの VLAN Tag 内にあるユーザ優先度に基づいて優先度を決定する機能です。本装置では，常にユーザ優先度マッピングが動作し，すべての受信フレームに対して優先度を決定します。

優先度の値には，装置内の優先度を表す CoS 値を用います。受信フレームのユーザ優先度の値から CoS 値にマッピングし，CoS 値によって送信キューを決定します。CoS 値と送信キューの対応については，「3.10.2 CoS マッピング機能」を参照してください。

ユーザ優先度は，VLAN Tag ヘッダ内タグ情報（Tag Control）の上位 3 ビットを示します。なお，VLAN Tag がないフレームは，常に CoS 値 3 を使用します。

フロー制御による優先度決定が動作する場合，ユーザ優先度マッピングよりも優先して動作します。

表 2-2 ユーザ優先度と CoS 値のマッピング

フレームの種類		マッピングされる CoS 値
VLAN Tag の有無	ユーザ優先度値	
VLAN Tag なし	—	3
VLAN Tag あり※	0	0
	1	1
	2	2
	3	3
	4	4
	5	5
	6	6
	7	7

（凡例）－：該当なし
注※　VLAN トンネリングまたは Tag 変換を設定したポートで受信したフレームは，受信時のユーザ優先度値に関係なく，常に CoS 値 3 にマッピングされます。

2.3 QoS 制御共通のコンフィグレーション

2.3.1 コンフィグレーションコマンド一覧

QoS 制御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 2-3 コンフィグレーションコマンド一覧

コマンド名	説明
ip qos-flow-group	イーサネットインタフェースまたは VLAN に対して，IPv4 QoS フローリストを適用し，IPv4 QoS 制御を有効にします。
ip qos-flow-list	IPv4 QoS フロー検出として動作する QoS フローリストを設定します。
ip qos-flow-list resequence	IPv4 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
ipv6 qos-flow-group	イーサネットインタフェースに対して，IPv6 QoS フローリストを適用し，IPv6 QoS 制御を有効にします。
ipv6 qos-flow-list	IPv6 QoS フロー検出として動作する QoS フローリストを設定します。
ipv6 qos-flow-list resequence	IPv6 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
mac qos-flow-group	イーサネットインタフェースまたは VLAN に対して，MAC QoS フローリストを適用し，MAC QoS 制御を有効にします。
mac qos-flow-list	MAC QoS フロー検出として動作する QoS フローリストを設定します。
mac qos-flow-list resequence	MAC QoS フローリストの条件適用順序のシーケンス番号を再設定します。
qos	QoS フローリストでのフロー検出条件および動作指定を設定します。
qos-queue-group	イーサネットインタフェースに対して，QoS キューリスト情報を適用し，レガシーシェーパを有効にします。
qos-queue-list	QoS キューリスト情報にスケジューリングモードを設定します。
remark	QoS の補足説明を記述します。
system ip-multicast-qos-assist	IP マルチキャストパケットフロー制御補助モードを設定します。
traffic-shape rate	イーサネットインタフェースにポート帯域制御を設定します。
flow detection mode ※	フィルタ・QoS 制御の受信側フロー検出モードを設定します。

注※

「コンフィグレーションコマンドレファレンス　22. フロー検出モード」を参照してください。

2.4 QoS 制御共通のオペレーション

2.4.1 運用コマンド一覧

QoS 制御共通の運用コマンド一覧を次の表に示します。

表 2-4 運用コマンド一覧

コマンド名	説明
show qos-flow	QoS フローグループコマンド (mac qos-flow-group，ip qos-flow-group，ipv6 qos-flow-group) で設定した QoS フローリスト (mac qos-flow-list，ip qos-flow-list，ipv6 qos-flow-list) の統計情報を表示します。
clear qos-flow	QoS フローグループコマンド (mac qos-flow-group，ip qos-flow-group，ipv6 qos-flow-group) で設定した QoS フローリスト (mac qos-flow-list，ip qos-flow-list，ipv6 qos-flow-list) の統計情報をクリアします。
show qos queueing	イーサネットインタフェースの送信キューの統計情報を表示します。
clear qos queueing	イーサネットインタフェースの送信キューの統計情報をクリアします。

3 フロー制御

この章では本装置のフロー制御（フロー検出，帯域監視，マーカー，優先度決定）について説明します。

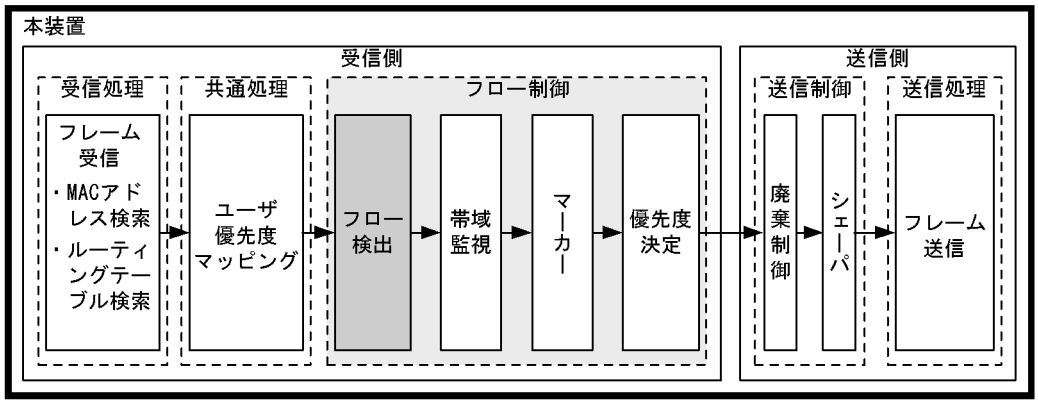
3.1 フロー検出解説

フロー検出とは，フレームの一連の流れであるフローを MAC ヘッダ，IP ヘッダ，TCP ヘッダ，ICMP ヘッダなどの条件に基づいてフレームを検出する機能です。QoS フローリストで設定します。QoS フローリストの詳細は，「3.1.3　QoS フローリスト」を参照してください。

本装置では，受信側イーサネットインタフェース・VLAN インタフェースで，イーサネット V2 形式および IEEE802.3 の SNAP/RFC1042 形式フレームのフロー検出ができます。設定可能なインタフェースは，受信側フロー検出モードによって変わります。なお，本装置宛ての受信フレームもフロー検出対象です。

この節で説明するフロー検出の位置づけを次の図に示します。

図 3-1　フロー検出の位置づけ



（凡例）：この節で説明するブロック

3.1.1 受信側フロー検出モード

本装置では，ネットワーク構成や運用形態を想定して受信側フロー検出モードを用意しています。使い方に合わせて選択してください。また，受信側フロー検出モードを選択する際の目安について次に示します。MAC 条件，IPv4 条件，および IPv6 条件の詳細は「3.1.2　フロー検出条件」を参照してください。

- MAC 条件でフレームを検出したい場合は，layer2-1 を使用してください。
- IPv4 条件に特化してフレームを検出したい場合は，layer2-2，layer2-5，および layer2-6 のどれかを使用してください。TCP/UDP ポート番号の範囲指定は layer2-5 および layer2-6 で指定可能です。
- IPv4 条件および IPv6 条件でフレームを検出したい場合は，layer2-3，layer2-4 のどちらかを使用してください。
- IPv4 条件でフレームを検出して，かつ DHCP snooping の端末フィルタを使用したい場合は，layer2-dhcp-1 を使用してください。

受信側フロー検出モードは flow detection mode コマンドで指定します。なお，選択した受信側フロー検出モードはフィルタ・QoS で共通です。

受信側フロー検出モードを指定しない場合，layer2-2 がデフォルトのモードとして設定されます。

受信側フロー検出モードとフロー動作の関係を次の表に示します。

表 3-1 受信側フロー検出モードとフロー動作の関係

受信側フロー検出モード	運用目的	フロー動作	検出対象インタフェース
layer2-1	IP パケットやそれ以外のフレームのフロー制御を行いたい場合に使用します。	MAC アドレス，イーサネットタイプなどの MAC ヘッダでフレームを検出します。	イーサネット，VLAN
layer2-2	IPv4 パケットに特化し，きめ細かいフロー制御を行いたい場合に使用します。	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。	イーサネット，VLAN
layer2-3	IPv4，IPv6 パケットに特化したフロー制御を行いたい場合に使用します。	IPv4 パケットは，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。 IPv6 パケットは，送信元 IP アドレスでフレームを検出します。	イーサネット
layer2-4	IPv4，IPv6 パケットに特化したフロー制御を行いたい場合に使用します。	IPv4 パケットは，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。 IPv6 パケットは，宛先 IP アドレスでフレームを検出します。	イーサネット
layer2-5	IPv4 パケットに特化し，きめ細かいフロー制御を行いたい場合に使用します。TCP/UDP ポート番号では範囲指定によるフロー検出ができます。宛先ポート番号を重視する場合に使用します。	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダでフレームを検出します。	イーサネット，VLAN
layer2-6	IPv4 パケットに特化し，きめ細かいフロー制御を行いたい場合に使用します。TCP/UDP ポート番号では範囲指定によるフロー検出が可能です。送信元ポート番号を重視する場合に使用します。	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。	イーサネット，VLAN
layer2-dhcp-1	IPv4 パケットに特化したフロー制御を行い，かつ DHCP snooping の端末フィルタを使用したい場合に使用します。	IPv4 パケットについて，IP ヘッダ，TCP/UDP ヘッダ，ICMP ヘッダでフレームを検出します。	イーサネット

3.1.2 フロー検出条件

フロー検出するためには，コンフィグレーションでフローを識別するための条件を指定します。受信側フロー検出モードごとの指定可能なフロー検出条件を次の表に示します。

表 3-2 指定可能なフロー検出条件（1/4）

種別		設定項目	layer2-1		layer2-2	
			イーサネット	VLAN	イーサネット	VLAN
MAC 条件	コンフィグレーション	VLAN ID ※1	○	－	－	－
	MAC ヘッダ	送信元 MAC アドレス	○	○	－	－

種別		設定項目		layer2-1		layer2-2	
				イーサネット	VLAN	イーサネット	VLAN
		宛先 MAC アドレス		○	○	－	－
		イーサネットタイプ		○	○	－	－
		ユーザ優先度※2		○	○	－	－
IPv4 条件	コンフィグレーション	VLAN ID※1		－	－	○	－
	MAC ヘッダ	ユーザ優先度※2		－	－	○	○
	IPv4 ヘッダ※3	上位プロトコル		－	－	○	○
		送信元 IP アドレス		－	－	○	○
		宛先 IP アドレス		－	－	○	○
		ToS		－	－	○	○
		DSCP		－	－	○	○
		Precedence		－	－	○	○
	IPv4-TCP ヘッダ	送信元ポート番号	単一指定（eq）	－	－	○	○
			範囲指定（range）	－	－	－	－
		宛先ポート番号	単一指定（eq）	－	－	○	○
			範囲指定（range）	－	－	－	－
		TCP 制御フラグ※4		－	－	○	○
	IPv4-UDP ヘッダ	送信元ポート番号	単一指定（eq）	－	－	○	○
			範囲指定（range）	－	－	－	－
		宛先ポート番号	単一指定（eq）	－	－	○	○
			範囲指定（range）	－	－	－	－
	IPv4-ICMP ヘッダ	ICMP タイプ値		－	－	○	○
		ICMP コード値		－	－	○	○
IPv6 条件	コンフィグレーション	VLAN ID※1		－	－	－	－
	MAC ヘッダ	ユーザ優先度※2		－	－	－	－
	IPv6 ヘッダ	送信元 IP アドレス		－	－	－	－
		宛先 IP アドレス		－	－	－	－

表 3-3 指定可能なフロー検出条件（2/4）

種別		設定項目		layer2-3	layer2-4
				イーサネット	イーサネット
MAC 条件	コンフィグレーション	VLAN ID※1		－	－
	MAC ヘッダ	送信元 MAC アドレス		－	－
		宛先 MAC アドレス		－	－
		イーサネットタイプ		－	－
		ユーザ優先度※2		－	－
IPv4 条件	コンフィグレーション	VLAN ID※1		○	○
	MAC ヘッダ	ユーザ優先度※2		○	○
	IPv4 ヘッダ※3	上位プロトコル		○	○
		送信元 IP アドレス		○	○
		宛先 IP アドレス		○	○
		ToS		○	○
		DSCP		○	○
		Precedence		○	○
	IPv4-TCP ヘッダ	送信元ポート番号	単一指定（eq）	○	○
			範囲指定（range）	－	－
		宛先ポート番号	単一指定（eq）	○	○
			範囲指定（range）	－	－
		TCP 制御フラグ※4		○	○
	IPv4-UDP ヘッダ	送信元ポート番号	単一指定（eq）	○	○
			範囲指定（range）	－	－
		宛先ポート番号	単一指定（eq）	○	○
			範囲指定（range）	－	－
	IPv4-ICMP ヘッダ	ICMP タイプ値		○	○
		ICMP コード値		○	○
IPv6 条件	コンフィグレーション	VLAN ID※1		○	○
	MAC ヘッダ	ユーザ優先度※2		○	○
	IPv6 ヘッダ	送信元 IP アドレス		○	－
		宛先 IP アドレス		－	○

表 3-4 指定可能なフロー検出条件（3/4）

種別		設定項目		layer2-5		layer2-6	
				イーサネット	VLAN	イーサネット	VLAN
MAC 条件	コンフィグレーション	VLAN ID※1		－	－	－	－
	MAC ヘッダ	送信元 MAC アドレス		－	－	－	－
		宛先 MAC アドレス		－	－	－	－
		イーサネットタイプ		－	－	－	－
		ユーザ優先度※2		－	－	－	－
IPv4 条件	コンフィグレーション	VLAN ID※1		○	－	○	－
	MAC ヘッダ	ユーザ優先度※2		○	○	○	○
	IPv4 ヘッダ※3	上位プロトコル		○	○	○	○
		送信元 IP アドレス		○	○	○	○
		宛先 IP アドレス		○	○	○	○
		ToS		○	○	○	○
		DSCP		○	○	○	○
		Precedence		○	○	○	○
	IPv4-TCP ヘッダ	送信元ポート番号	単一指定（eq）	○※5	○※5	○	○
			範囲指定（range）	○※5	○※5	○※5	○※5
		宛先ポート番号	単一指定（eq）	○	○	○※5	○※5
			範囲指定（range）	○※5	○※5	○※5	○※5
		TCP 制御フラグ※4		○	○	○	○
	IPv4-UDP ヘッダ	送信元ポート番号	単一指定（eq）	○※5	○※5	○	○
			範囲指定（range）	○※5	○※5	○※5	○※5
		宛先ポート番号	単一指定（eq）	○	○	○※5	○※5
			範囲指定（range）	○※5	○※5	○※5	○※5
	IPv4-ICMP ヘッダ	ICMP タイプ値		－	－	○	○
		ICMP コード値		－	－	○	○
IPv6 条件	コンフィグレーション	VLAN ID※1		－	－	－	－
	MAC ヘッダ	ユーザ優先度※2		－	－	－	－
	IPv6 ヘッダ	送信元 IP アドレス		－	－	－	－
		宛先 IP アドレス		－	－	－	－

表 3-5 指定可能なフロー検出条件（4/4）

種別		設定項目		layer2-dhcp-1
				イーサネット
MAC 条件	コンフィグレーション	VLAN ID※1		－
	MAC ヘッダ	送信元 MAC アドレス		－
		宛先 MAC アドレス		－
		イーサネットタイプ		－
		ユーザ優先度※2		－
IPv4 条件	コンフィグレーション	VLAN ID※1		○
	MAC ヘッダ	ユーザ優先度※2		○
	IPv4 ヘッダ※3	上位プロトコル		○
		送信元 IP アドレス		○
		宛先 IP アドレス		○
		ToS		○
		DSCP		○
		Precedence		○
	IPv4-TCP ヘッダ	送信元ポート番号	単一指定（eq）	○
			範囲指定（range）	－
		宛先ポート番号	単一指定（eq）	○
			範囲指定（range）	－
		TCP 制御フラグ※4		○
	IPv4-UDP ヘッダ	送信元ポート番号	単一指定（eq）	○
			範囲指定（range）	－
		宛先ポート番号	単一指定（eq）	○
			範囲指定（range）	－
	IPv4-ICMP ヘッダ	ICMP タイプ値		○
		ICMP コード値		○
IPv6 条件	コンフィグレーション	VLAN ID※1		－
	MAC ヘッダ	ユーザ優先度※2		－
	IPv6 ヘッダ	送信元 IP アドレス		－
		宛先 IP アドレス		－

（凡例）○：指定できる　　－：指定できない

注※ 1

本装置のフロー検出で検出できる VLAN ID は，VLAN コンフィグレーションで入力した VLAN に対して付与する値です。入力フレームの属する VLAN ID を検出します。

注※ 2

次に示すフレームについてはユーザ優先度を検出できません。常に，ユーザ優先度 3 として検出します。

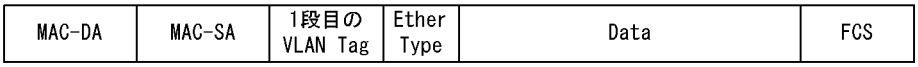
・VLAN Tag なしのフレーム

・VLAN トンネリングを設定したポートで受信したフレーム

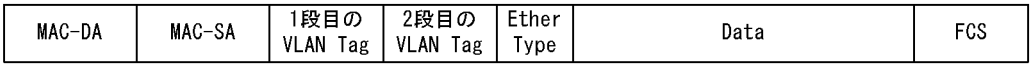
・Tag 変換機能により Tag 変換されたフレーム

VLAN Tag が複数あるフレームに対してユーザ優先度を検出する場合，MAC アドレス側から 1 段目の VLAN Tag にあるユーザ優先度が対象となります。次の図に VLAN Tag が複数あるフレームの例を示します。

（i）VLAN Tag 1段のフォーマット



（ii）VLAN Tag 2段のフォーマット

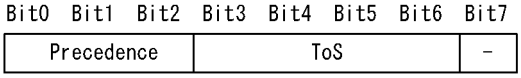


注※ 3

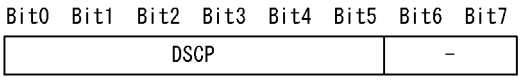
ToS フィールドの指定についての補足

ToS　　：ToS フィールドの 3 ビット～ 6 ビットの値です。

Precedence：ToS フィールドの上位 3 ビットの値です。



DSCP　　：ToS フィールドの上位 6 ビットの値です。



注※ 4

ack/fin/psh/rst/syn/urg フラグが 1 のパケットを検出します。

注※ 5

ハードウェアリソースである TCP/UDP ポート番号検出パターンを使用します。TCP/UDP ポート番号検出パターンの使用例については，マニュアル「コンフィグレーションガイド Vol.1　3.2.4 フィルタ・QoS」を参照してください。

3.1.3　QoS フローリスト

QoS のフロー検出を実施するためにはコンフィグレーションで QoS フローリストを設定します。フロー検出条件に応じて設定する QoS フローリストが異なります。また，フロー検出条件ごとに検出可能なフレーム種別が異なります。フロー検出条件と対応する QoS フローリスト，および検出可能なフレーム種別の関係を次の表に示します。

表 3-6 フロー検出条件と対応する QoS フローリスト，検出可能なフレーム種別の関係

フロー検出条件	対応する QoS フローリスト	対応する受信側フロー検出モード	検出可能なフレーム種別		
			非 IP	IPv4	IPv6
MAC 条件	mac qos-flow-list	layer2-1	○	○	○
IPv4 条件	ip qos-flow-list	layer2-2, layer2-3, layer2-4, layer2-5, layer2-6, layer2-dhcp-1	―	○	―
IPv6 条件	ipv6 qos-flow-list	layer2-3, layer2-4	―	―	○

（凡例）○：検出できる　　―：検出できない

QoS フローリストのインタフェースへの適用は，QoS フローグループコマンドで実施します。適用順序は，QoS フローリストのパラメータであるシーケンス番号によって決定します。また，QoS フローリストごとに，QoS エントリの検索は独立して実施します。そのため，フレームが複数の QoS エントリに一致することがあります。複数の QoS エントリに一致した場合，実際に動作するのは単一の QoS エントリです。

（1） イーサネットインタフェースと VLAN インタフェース同時に一致した場合の動作

イーサネットインタフェースと，該当するイーサネットインタフェースが属する VLAN インタフェースに対して QoS エントリを設定し，該当するイーサネットインタフェースからの受信フレームに対して QoS フロー検出を実施すると，複数の QoS エントリに一致する場合があります。イーサネットインタフェースおよび VLAN インタフェースの QoS エントリに一致する場合は，イーサネットインタフェース上の QoS エントリを優先します。複数の QoS エントリに一致した場合の動作を次の表に示します。

表 3-7 複数の QoS エントリに一致した場合の動作

複数 QoS エントリ一致となる組み合わせ		有効になる QoS エントリ
イーサネット	VLAN	
○	―	イーサネット
―	○	VLAN
○	○	イーサネット

（凡例）○：指定あり　　―：指定なし

この条件に該当する受信側フロー検出モードは，layer2-1，layer2-2，layer2-5，layer2-6 です。

3.1.4 フロー検出使用時の注意事項

（1） 複数 QoS エントリ一致時の動作

フレームが複数の QoS エントリに一致した場合，一致した QoS エントリの統計情報が採られます。

（2） VLAN-Tag 付きフレームに対する QoS フロー検出

3 段以上の VLAN-Tag があるフレームに対して，MAC 条件のイーサネットタイプ，IPv4 条件，または IPv6 条件をフロー検出条件とした QoS フロー検出を実施できません。

2 段の VLAN-Tag があるフレームに対して，MAC 条件のイーサネットタイプ，IPv4 条件，または IPv6 条件をフロー検出条件とした QoS フロー検出を実施するためには，次の条件をすべて満たす必要があります。

- 本装置のどれかのポートで，VLAN トンネリング機能または Tag 変換機能が動作している
- フレームを受信したポートが，Tag 変換機能が動作していないトランクポートである

（3） IPv4 フラグメントパケットに対する QoS フロー検出

IPv4 フラグメントパケットに対して TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件とした QoS フロー検出を行った場合，2 番目以降のフラグメントパケットは TCP/UDP ヘッダ・ICMP ヘッダがフレーム内にないため検出できません。フラグメントパケットを含めた QoS フロー検出を実施する場合は，フロー検出条件に MAC ヘッダ，IP ヘッダを指定してください。

（4） QoS エントリ変更時の動作

本装置では，インタフェースに適用済みの QoS エントリを変更すると，変更が反映されるまでの間，検出の対象となるフレームが検出されなくなります。そのため，一時的にほかの QoS エントリで検出される場合があります。

（5） ほかの機能との同時動作

以下の場合フレームは廃棄しますが，インタフェースに対して QoS エントリを設定し一致した場合，一致した QoS エントリの統計情報が採られます。

- VLAN のポートのデータ転送状態が Blocking（データ転送停止中）の状態で，該当ポートからフレームを受信した場合
- プロトコル VLAN・MAC VLAN で，VLAN-Tag 付きフレームを受信した場合
- ポート間中継遮断機能で指定したポートからフレームを受信した場合
- ネイティブ VLAN をトランクポートで送受信する VLAN に設定しないで，VLAN-Tag なしフレームを受信した場合
- トランクポートで送受信する VLAN に設定していない VLAN-Tag 付きフレームを受信した場合
- アクセスポートで VLAN-Tag 付きフレームを受信した場合
- 廃棄動作を指定したフィルタエントリ（暗黙の廃棄のエントリを含む）に一致するフレームを受信した場合

インタフェースに対して QoS エントリを設定しフレームが一致した場合，次の動作は無効になります。

- DHCP snooping の端末フィルタによるフレーム廃棄
- 認証専用 IPv4 アクセスリストによるフレーム廃棄

3.2 フロー検出コンフィグレーション

3.2.1 受信側フロー検出モードの設定

QoS 制御の受信側フロー検出モードを指定する例を示します。

[設定のポイント]

受信側フロー検出モードは，ハードウェアの基本的な動作条件を決定するため，最初に設定します。

[コマンドによる設定]

1. **(config)# flow detection mode layer2-3**
   受信側フロー検出モード layer2-3 を有効にします。

3.2.2 複数インタフェースの QoS 制御の指定

複数のイーサネットインタフェースに QoS 制御を指定する例を示します。

[設定のポイント]

config-if-range モードで QoS 制御を有効に設定することで，複数のイーサネットインタフェースに QoS 制御を設定できます。

[コマンドによる設定]

1. **(config)# ip qos-flow-list QOS-LIST1**
   IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.168.100.10 action cos 6**
   192.168.100.10 の IP アドレスを宛先とし，CoS 値＝ 6 の QoS フローリストを設定します。

3. **(config-ip-qos)# exit**
   IPv4 QoS フローリストモードから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 range gigabitethernet 0/1-4**
   ポート 0/1-4 のインタフェースモードに移行します。

5. **(config-if-range)# ip qos-flow-group QOS-LIST1 in**
   受信側に IPv4 QoS フローリストを有効にします。

3.2.3 TCP/UDP ポート番号の範囲で QoS 制御する設定

UDP ポート番号の範囲をフロー検出条件とし，QoS 制御を設定する例を示します。

[設定のポイント]

フレーム受信時に UDP ヘッダの宛先ポート番号の範囲によってフロー検出を行い，QoS 制御を実施します。

［コマンドによる設定］

1. **(config)# ip qos-flow-list QOS-LIST1**
   IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos udp any any range 10 20 action cos 6**
   UDP ヘッダの宛先ポート番号の範囲 10 ～ 20 をフロー検出条件とし，CoS 値＝ 6 の QoS フローリストを設定します。

3. **(config-ip-qos)# exit**
   IPv4 QoS フローリストモードから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 gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

5. **(config-if)# ip qos-flow-group QOS-LIST1 in**
   受信側に IPv4 QoS フローリストを有効にします。

3.3 フロー検出のオペレーション

show qos-flow コマンドによって，設定した内容が反映されているかどうかを確認します。

3.3.1 IPv4 パケットをフロー検出条件とした QoS 制御の動作確認

IPv4 パケットをフロー検出条件とした QoS 制御の動作確認の方法を次の図に示します。

図 3-2 IPv4 パケットをフロー検出条件とした QoS 制御の動作確認

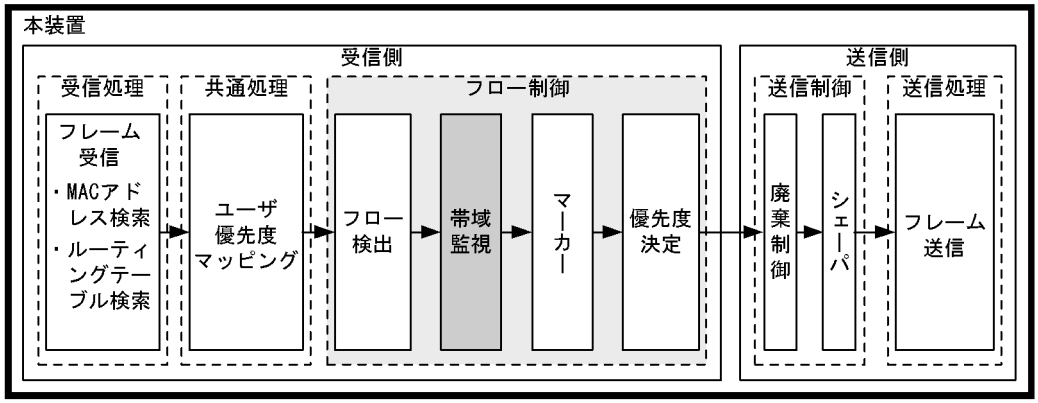
```
> show qos-flow 0/1
Date 2005/12/01 12:00:00 UTC
Using Port:0/1 in
IP qos-flow-list:QOS-LIST1
      ip any host 192.168.100.10 action replace-user-priority 6
         matched packets       :  74699826
```

指定したポートの QoS 制御に「IP qos-flow-list」が表示されることを確認します。

3.4 帯域監視解説

帯域監視は，フロー検出で検出したフローの帯域を監視する機能です。この節で説明する帯域監視の位置づけを次の図に示します。

図 3-3 帯域監視の位置づけ



（凡例）：この節で説明するブロック

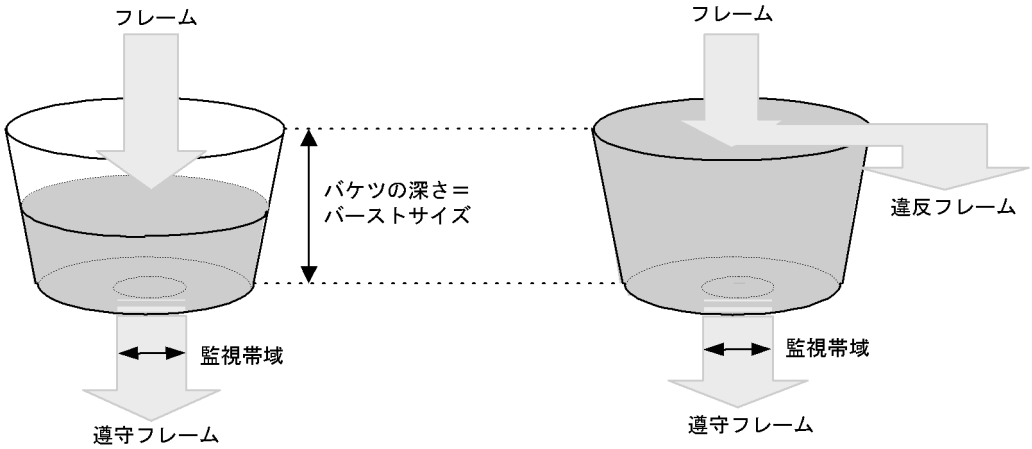
3.4.1 帯域監視

フロー検出で検出したフレームのフレーム長（MAC アドレスから FCS まで）を基に帯域を監視する機能です。指定した監視帯域内として中継するフレームを「遵守フレーム」，監視帯域以上としてペナルティを科すフレームを「違反フレーム」と呼びます。

フロー検出で検出したフレームが監視帯域を遵守しているかまたは違反しているかの判定には，水の入った穴の開いたバケツをモデルとする，Leaky Bucket アルゴリズムを用いています。

Leaky Bucket アルゴリズムのモデルを次の図に示します。

図 3-4 Leaky Bucket アルゴリズムのモデル



バケツからは監視帯域分の水が流れ，フレーム受信時には MAC アドレスから FCS までのサイズの水が注ぎ込まれます。水が注ぎ込まれる際にバケツがあふれていなければ，遵守フレームとして中継されます（上図の左側の例）。水が注ぎ込まれる際にバケツがあふれている場合は，フロー検出で検出したフレーム

を違反フレームとしてペナルティを科します（上図の右側の例）。水が一時的に大量に注ぎこまれたときに許容できる量，すなわちバケツの深さがバーストサイズに対応します。

バーストサイズのデフォルトは 16kbyte ですが，より帯域の揺らぎが大きいトラフィックの遵守パケットを中継する際には，バッファサイズを大きく設定し使用してください。

本機能は，最低帯域監視と最大帯域制御から成り，最低帯域監視と最大帯域制御で使用できるペナルティの種類を次の表に示します。

表 3-8　最低帯域監視と最大帯域制御で使用できるペナルティの種類

違反フレームに対するペナルティ	帯域監視種別	
	最低帯域監視	最大帯域制御
廃棄	―	○
キューイング優先度変更	○	―
DSCP 書き換え	○	―

（凡例）○：使用可能なペナルティ　　―：使用不可能なペナルティ

次のフレームについては，キューイング優先度変更および DSCP 書き換えのペナルティが動作しません。

- MTU を超える IPv4，IPv6 パケット
- TTL が 1 のフレーム
- ホップリミットが 1 のフレーム
- IP オプション付きのフレーム
- IPv6 拡張ヘッダ付きのフレーム
- 宛先不明の IPv4，IPv6 パケット

3.4.2　帯域監視使用時に採取可能な統計情報

帯域監視ごとに採取可能な統計情が異なります。帯域監視使用時に採取可能な統計情報を次の表に示します。

表 3-9　帯域監視使用時に採取可能な統計情報

帯域監視種別	採取可能な統計情報			
	最大帯域違反	最大帯域遵守	最低帯域違反	最低帯域遵守
最低帯域監視	―	―	○	○
最大帯域制御	○	○	―	―
最低帯域監視と最大帯域制御の組み合わせ	○	○	―	―

（凡例）○：採取可能　　―：採取不可能

3.4.3　帯域監視使用時の注意事項

(1) フローで指定した監視帯域と出力回線・出力キューの関係

複数のフローで帯域監視機能を使用している場合，各 QoS フローエントリで指定した監視帯域値の合計が，出力イーサネットインタフェース，または送信キューの帯域値以内となるように，各監視帯域値を調整してください。

(2) 帯域監視機能を使用しないフローとの混在

帯域監視機能を使用しないフローと使用するフローが同じ回線またはキューに出力されないようにしてください。

(3) プロトコル制御フレームの帯域監視

本装置では，本装置宛てのプロトコル制御フレームも帯域監視対象になります。したがって，本装置宛てのプロトコル制御フレームも最大帯域制御違反として廃棄される場合があります。そのため，本装置宛てのプロトコル制御フレームを考慮した最大帯域を確保する必要があります。

(4) TCP フレームに対する最大帯域制御の使用

最大帯域制御を使用した場合には，TCP のスロースタートが繰り返されデータ転送速度が極端に遅くなる場合があります。

上記動作を防ぐために，最低帯域監視を使用して，「フレームが廃棄されやすくなるようにキューイング優先度を下げる」の動作を実施するようにしてください。本設定によって，契約帯域を超えてもすぐに廃棄されないで，出力回線が混んできたときだけに廃棄されるようになります。

(5) VLAN インタフェースに対する帯域監視機能の使用

次に示すモデルでは，イーサネットインタフェース 0/1 ～ 0/24 とイーサネットインタフェース 0/25 ～ 0/48 をまたがった VLAN インタフェースに対して帯域監視を使用しないでください。

- AX2430S-48T
- AX2430S-48TD

次に示すモデルでは，イーサネットインタフェース 0/1 ～ 0/24，0/49，0/50 と，イーサネットインタフェース 0/25 ～ 0/48 をまたがった VLAN インタフェースに対して帯域監視を使用しないでください。

- AX2430S-48T2X

(6) ほかの機能との同時動作

次に示す場合，フレームは廃棄しますが帯域監視対象になります。

- 廃棄動作を指定したフィルタエントリ（暗黙の廃棄のエントリを含む）に一致するフレームを受信した場合

3.5 帯域監視のコンフィグレーション

3.5.1 最大帯域制御の設定

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，最大帯域制御を行う帯域監視を設定します。

[コマンドによる設定]

1. **(config)#ip qos-flow-list QOS-LIST1**
   IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)#qos ip any host 192.168.100.10 action max-rate 5M max-rate-burst 512**
   宛先 IP アドレスが 192.168.100.10 のフローに対し，最大帯域制御の監視帯域 =5Mbit/s，最大帯域制御のバーストサイズ =512kbyte の IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)#exit**
   IPv4 QoS フローリストモードから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 gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

5. **(config-if)#ip qos-flow-group QOS-LIST1 in**
   受信側に IPv4 QoS フローリスト（QOS-LIST1）を有効にします。

3.5.2 最低帯域監視違反時のキューイング優先度の設定

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，最低帯域監視を行うことを設定します。最低帯域監視を違反したフレームに対しては，キューイング優先度の変更を行う設定をします。

[コマンドによる設定]

1. **(config)#ip qos-flow-list QOS-LIST2**
   IPv4 QoS フローリスト（QOS-LIST2）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)#qos ip any host 192.168.110.10 action min-rate 1M min-rate-burst 64 penalty-discard-class 1**
   宛先 IP アドレスが 192.168.110.10 のフローに対し，最低監視帯域 =1Mbit/s，最低監視帯域のバーストサイズ =64kbyte，最低帯域監視での違反フレームのキューイング優先度 =1 の IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)#exit**
   IPv4 QoS フローリストモードから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 gigabitethernet 0/3**
   ポート 0/3 のインタフェースモードに移行します。

5. **(config-if)#ip qos-flow-group QOS-LIST2 in**
   受信側に IPv4 QoS フローリスト（QOS-LIST2）を有効にします。

3.5.3 最低帯域監視違反時の DSCP 書き換えの設定

特定のフローに対して最低帯域監視（違反フレームは DSCP の書き換え）を実施する場合に設定します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，最低帯域監視（min-rate）を行う帯域監視を設定します。最低監視帯域を違反したフレームに対しては，DSCP 値の変更を行う設定をします。

[コマンドによる設定]

1. **(config)#ip qos-flow-list QOS-LIST3**
   IPv4 QoS フローリスト（QOS-LIST3）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)#qos ip any host 192.168.120.10 action min-rate 1M min-rate-burst 64 penalty-dscp 8**
   宛先 IP アドレスが 192.168.120.10 のフローに対し，最低監視帯域 =1Mbit/s，最低監視帯域のバーストサイズ =64kbyte，最低帯域監視での違反フレームの DSCP 値 =8 の IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)#exit**
   IPv4 QoS フローリストモードから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 gigabitethernet 0/5**
   ポート 0/5 のインタフェースモードに移行します。

5. **(config-if)#ip qos-flow-group QOS-LIST3 in**
   受信側に IPv4 QoS フローリスト（QOS-LIST3）を有効にします。

3.5.4 最大帯域制御と最低帯域監視の組み合わせの設定

特定のフローに対して最大帯域制御と最低帯域監視（違反フレームは DSCP の書き換え）を実施したい場合に設定します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，最大帯域制御と最低帯域監視を行う帯域監視を設定します。最低帯域監視を違反したフレームに対しては，DSCP 値の変更を行う設定をします。

[コマンドによる設定]

1. **(config)#ip qos-flow-list QOS-LIST4**
   IPv4 QoS フローリスト（QOS-LIST4）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)#qos ip any host 192.168.130.10 action max-rate 5M max-rate-burst 512 min-rate 1M min-rate-burst 64 penalty-dscp 8**
   宛先 IP アドレスが 192.168.130.10 のフローに対し，最大帯域制御の監視帯域 =5Mbit/s，最大帯域制御のバーストサイズ =512kbyte，最低監視帯域 =1Mbit/s，最低監視帯域のバーストサイズ =64kbyte，最低帯域監視での違反フレームの DSCP 値 =8 の IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)#exit**
   IPv4 QoS フローリストモードから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 gigabitethernet 0/7**
   ポート 0/7 のインタフェースモードに移行します。

5. **(config-if)#ip qos-flow-group QOS-LIST4 in**
   受信側に IPv4 QoS フローリスト（QOS-LIST4）を有効にします。

3.6 帯域監視のオペレーション

show qos-flow コマンドによって，設定した内容が反映されているかどうかを確認します。

3.6.1 最大帯域制御の確認

最大帯域制御の確認方法を次の図に示します。

図 3-5 最大帯域制御の確認

```
> show qos-flow 0/1

Date 2005/12/01 13:00:00 UTC
Using Port:0/1 in
IP qos-flow-list:QOS-LIST1
      ip any host 192.168.100.10 action max-rate 5M max-rate-burst 512
         matched packets(max-rate over) :         7
         matched packets(max-rate under):        28
>
```

QOS-LIST1 のリスト情報に「最大帯域制御の監視帯域（max-rate 5M）」，「最大帯域制御のバーストサイズ（max-rate-burst 512）」が表示されることを確認します。

3.6.2 最低帯域監視違反時のキューイング優先度の確認

最低帯域監視違反時のキューイング優先度の確認方法を次の図に示します。

図 3-6 最低帯域監視違反時のキューイング優先度の確認

```
> show qos-flow 0/3

Date 2005/12/01 13:00:00 UTC
Using Port:0/3 in
IP qos-flow-list:QOS-LIST2
      ip any host 192.168.110.10 action min-rate 1M min-rate-burst 64
penalty-discard-class 1
         matched packets(min-rate over) :      9826
         matched packets(min-rate under):  74699826
>
```

QOS-LIST2 のリスト情報に「最低監視帯域（min-rate 1M）」，「最低監視帯域のバーストサイズ（min-rate-burst 64）」，「違反フレームのキューイング優先度（penalty-discard-class 1）」が表示されることを確認します。

3.6.3 最低監視帯域違反時の DSCP 書き換えの確認

最低監視帯域違反時の DSCP 書き換えの確認方法を次の図に示します。

図 3-7 最低監視帯域違反時の DSCP 書き換えの確認

```
> show qos-flow 0/5

Date 2005/12/01 13:00:00 UTC
Using Port:0/5 in
IP qos-flow-list:QOS-LIST3
     ip any host 192.168.110.10 action min-rate 1M min-rate-burst 64 penalty-dscp
```

```
CS1
         matched packets(min-rate over) :        28
         matched packets(min-rate under):         7
>
```

QOS-LIST3 のリスト情報に「最低監視帯域（min-rate 1M）」,「最低監視帯域のバーストサイズ（min-rate-burst 64）」,「違反フレームの DSCP 値（penalty-dscp 8）」が表示されることを確認します。

3.6.4 最大帯域制御と最低帯域監視の組み合わせの確認

最大帯域制御と最低帯域監視の組み合わせの確認方法を次の図に示します。

図 3-8 最大帯域制御と最低帯域監視の組み合わせの確認

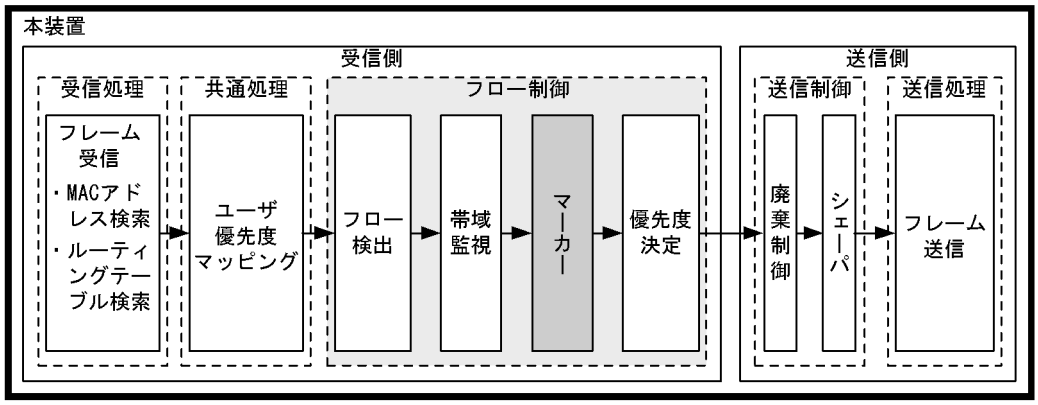
```
> show qos-flow 0/7

Date 2005/12/01 13:00:00 UTC
Using Port:0/7 in
IP qos-flow-list:QOS-LIST4
      ip any host 192.168.130.10 action max-rate 5M max-rate-burst 512 min-rate
1M min-rate-burst 64 penalty-dscp CS1
         matched packets(max-rate over) :  74699826
         matched packets(max-rate under):        28
>
```

QOS-LIST4 のリスト情報に「最大帯域制御の監視帯域（max-rate 5M）」,「最大帯域制御のバーストサイズ（max-rate-burst 512）」,「最低監視帯域（min-rate 1M）」,「最低監視帯域のバーストサイズ（min-rate-burst 64）」,「違反フレームの DSCP 値（penalty-dscp 8）」が表示されることを確認します。

3.7 マーカー解説

マーカーは，フロー検出で検出したフレームの VLAN Tag 内のユーザ優先度および IP ヘッダ内の DSCP を書き換える機能です。この節で説明するマーカーの位置づけを次の図に示します。

図 3-9 マーカーの位置づけ

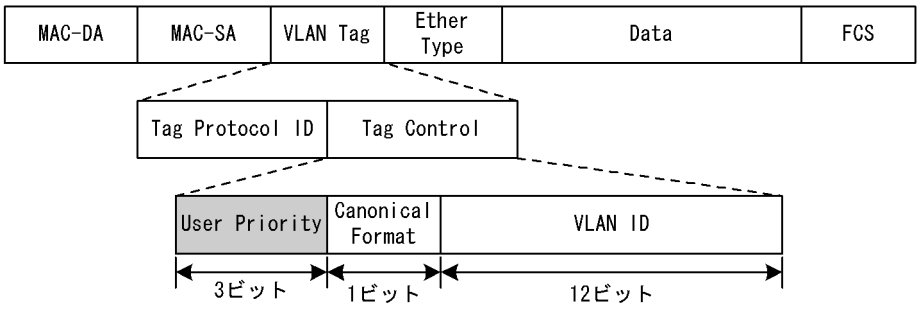


（凡例）：この節で説明するブロック

3.7.1 ユーザ優先度書き換え

フロー検出で検出したフレームの VLAN Tag 内にあるユーザ優先度（User Priority）を書き換える機能です。ユーザ優先度は，次の図に示すタグ情報（Tag Control）フィールドの先頭 3 ビットを指します。

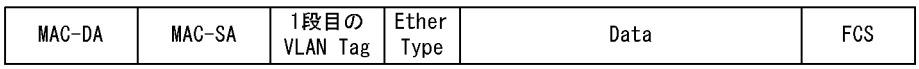
図 3-10 VLAN Tag のヘッダフォーマット



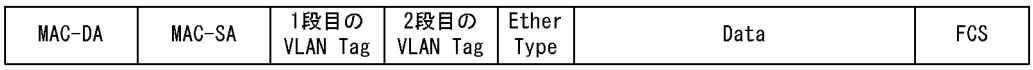
VLAN Tag が複数あるフレームに対してユーザ優先度書き換えを行う場合，MAC アドレス側から 1 段目の VLAN Tag にあるユーザ優先度を書き換えます。次の図に VLAN Tag が複数あるフレームフォーマットを示します。

図 3-11 VLAN Tag が複数あるフレームフォーマットの概略図

（i）VLAN Tag 1段のフォーマット



（ii）VLAN Tag 2段のフォーマット



次のフレームについてはユーザ優先度を書き換えることができません。

- VLAN トンネリングを設定したポートで送信するフレーム
- MTU を超える IPv4，IPv6 パケット
- TTL が 1 のフレーム
- ホップリミットが 1 のフレーム
- IP オプション付きのフレーム
- IPv6 拡張ヘッダ付きのフレーム
- 宛先不明の IPv4，IPv6 パケット

ユーザ優先度書き換えは，ユーザ優先度引き継ぎと同時に設定することはできません。

ユーザ優先度書き換えおよびユーザ優先度引き継ぎをどちらも実施しない場合は，次の表に示すユーザ優先度となります。

表 3-10　フレーム送信時のユーザ優先度

フレーム送信時のユーザ優先度	対象となるフレーム
3	• VLAN Tag なしで受信し，VLAN Tag ありで送信するフレーム • VLAN トンネリング機能で，アクセス回線からバックボーン回線に中継するフレーム • Tag 変換を設定したポートで受信し，Tag 変換されたフレーム
受信フレームのユーザ優先度	• VLAN トンネリング機能で，アクセス回線からアクセス回線に中継する VLAN Tag ありフレーム • Tag 変換を設定してない，かつ VLAN トンネリングを設定していないポートで VLAN Tag ありフレームを受信し，VLAN Tag ありで送信するフレーム

ユーザ優先度書き換えを優先度決定機能と同時に設定した場合，優先度決定機能で決定した CoS 値に応じて固定的にユーザ優先度を決定します。

優先度決定機能とユーザ優先度書き換え機能を同時に設定した場合のユーザ優先度を次の表に示します。

表 3-11　優先度決定機能とユーザ優先度書き換え機能を同時に設定した場合のユーザ優先度

優先度決定機能で決定した CoS 値	ユーザ優先度
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

3.7.2　ユーザ優先度引き継ぎ

VLAN トンネリング機能で，アクセス回線からのフレームに VLAN Tag を追加してバックボーン回線に中継するときに，フロー検出で検出したフレームのユーザ優先度を，バックボーン回線のユーザ優先度（追加する VLAN Tag のユーザ優先度）および優先度決定機能の CoS 値に引き継ぐ機能です。

ユーザ優先度引き継ぎは，VLAN トンネリングを設定したイーサネットインタフェースに設定できます。

ユーザ優先度引き継ぎを設定した場合の動作について，次の表に示します。

表 3-12 ユーザ優先度引き継ぎ機能を設定した場合の動作

フロー検出で検出したフレームのユーザ優先度	送信フレーム	
	ユーザ優先度	CoS 値
VLAN Tag なし	0	0
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7

ユーザ優先度引き継ぎは，ユーザ優先度書き換え機能および優先度決定機能（CoS 値の指定）と同時に設定することはできません。

ユーザ優先度引き継ぎを設定しない場合の CoS 値については「3.10.1 CoS 値・キューイング優先度」を，ユーザ優先度については「3.7.1 ユーザ優先度書き換え」を参照してください。

3.7.3 DSCP 書き換え

IPv4 ヘッダの TOS フィールドまたは IPv6 ヘッダのトラフィッククラスフィールドの上位 6 ビットである DSCP 値を書き換える機能です。TOS フィールドのフォーマットおよびトラフィッククラスフィールドのフォーマットの図を次に示します。

図 3-12 TOS フィールドのフォーマット

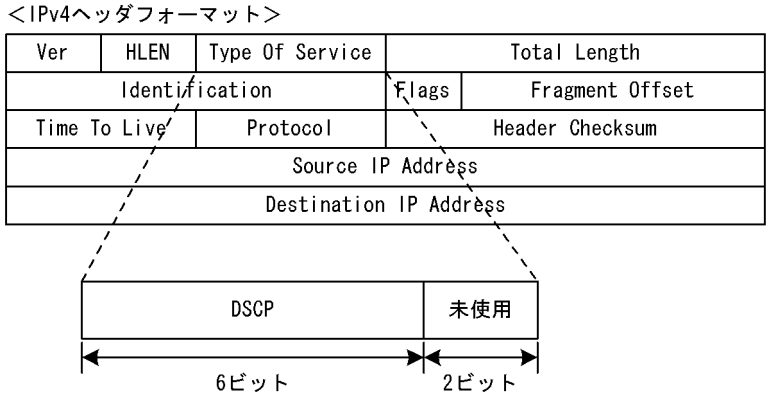
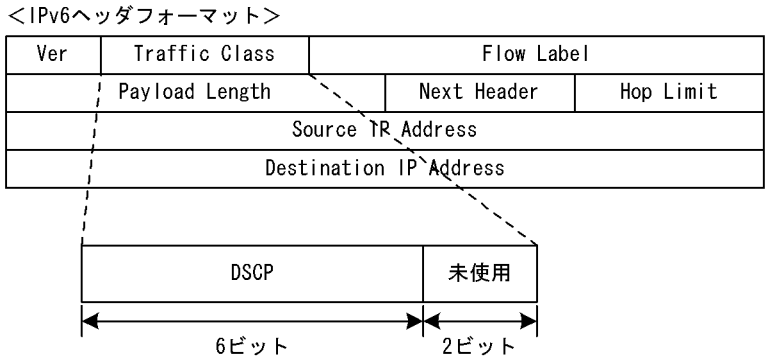


図 3-13　トラフィッククラスフィールドのフォーマット



検出したフローの TOS フィールドまたはトラフィッククラスフィールドの上位 6 ビットを書き換えます。

また，帯域監視からの指示によって，最低監視帯域を超えたフローの DSCP を書き換えることができます。例えば，最低監視帯域を超えたフローに対して，DSCP 値を 0 に設定できます。

最低帯域監視と同時に設定した場合の違反フレームの動作については，違反時のペナルティ指定動作が優先されます。

次のフレームについては DSCP を書き換えることができません。

- MTU を超える IPv4，IPv6 パケット
- TTL が 1 のフレーム
- ホップリミットが 1 のフレーム
- IP オプション付きのフレーム
- IPv6 拡張ヘッダ付きのフレーム
- 宛先不明の IPv4，IPv6 パケット

3.8 マーカーのコンフィグレーション

3.8.1 ユーザ優先度書き換えの設定

特定のフローに対してユーザ優先度を書き換える場合に設定します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，ユーザ優先度の書き換えを設定します。

[コマンドによる設定]

1. **(config)#ip qos-flow-list QOS-LIST1**
   IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)#qos ip any host 192.168.100.10 action replace-user-priority 6**
   192.168.100.10 の IP アドレスを宛先とし，ユーザ優先度を 6 に書き換える IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)#exit**
   IPv4 QoS フローリストモードから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 gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

5. **(config-if)#ip qos-flow-group QOS-LIST1 in**
   受信側の IPv4 QoS フローリスト（QOS-LIST1）を有効にします。

3.8.2 ユーザ優先度引き継ぎの設定

特定のフローに対してユーザ優先度引き継ぎを行う場合に設定します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，ユーザ優先度引き継ぎを行います。

[コマンドによる設定]

1. **(config)#ip qos-flow-list QOS-LIST2**
   IPv4 QoS フローリスト（QOS-LIST2）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)#qos ip any host 192.168.100.10 action copy-user-priority**
   192.168.100.10 の IP アドレスを宛先とし，ユーザ優先度引き継ぎを行う IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)#exit**
   IPv4 QoS フローリストモードから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 gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

5. **(config-if)#ip qos-flow-group QOS-LIST2 in**
   受信側の IPv4 QoS フローリスト（QOS-LIST2）を有効にします。

3.8.3 DSCP 書き換えの設定

特定のフローに対して DSCP を書き換える場合に設定します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，DSCP 値の書き換えを設定します。

[コマンドによる設定]

1. **(config)#ip qos-flow-list QOS-LIST3**
   IPv4 QoS フローリスト（QOS-LIST3）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)#qos ip any host 192.168.100.10 action replace-dscp 63**
   192.168.100.10 の IP アドレスを宛先とし，DSCP 値を 63 に書き換える IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)#exit**
   IPv4 QoS フローリストモードから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 gigabitethernet 0/3**
   ポート 0/3 のインタフェースモードに移行します。

5. **(config-if)#ip qos-flow-group QOS-LIST3 in**
   受信側の IPv4 QoS フローリスト（QOS-LIST3）を有効にします。

3.9 マーカーのオペレーション

show qos-flow コマンドによって，設定した内容が反映されているかどうかを確認します。

3.9.1 ユーザ優先度書き換えの確認

ユーザ優先度書き換えの確認方法を次の図に示します。

図 3-14 ユーザ優先度書き換えの確認

```
> show qos-flow 0/1

Date 2005/12/01 13:00:00 UTC
Using Port:0/1 in
IP qos-flow-list:QOS-LIST1
      ip any host 192.168.100.10 action replace-user-priority 6
         matched packets                        :       0
>
```

QOS-LIST1 のリスト情報に「replace-user-priority 6」が表示されることを確認します。

3.9.2 ユーザ優先度引き継ぎの確認

ユーザ優先度引き継ぎの確認方法を次の図に示します。

図 3-15 ユーザ優先度引き継ぎの確認

```
> show qos-flow 0/1

Date 2007/03/01 13:00:00 UTC
Using Port:0/1 in
IP qos-flow-list:QOS-LIST2
      ip any host 192.168.100.10 action copy-user-priority
         matched packets                        :       0
>
```

QOS-LIST2 のリスト情報に「copy-user-priority」が表示されることを確認します。

3.9.3 DSCP 書き換えの確認

DSCP 書き換えの確認方法を次の図に示します。

図 3-16 DSCP 書き換えの確認

```
> show qos-flow 0/3

Date 2005/12/01 13:00:00 UTC
Using Port:0/3 in
IP qos-flow-list:QOS-LIST3
      ip any host 192.168.100.10 action replace-dscp 63
         matched packets                        :       0
>
```

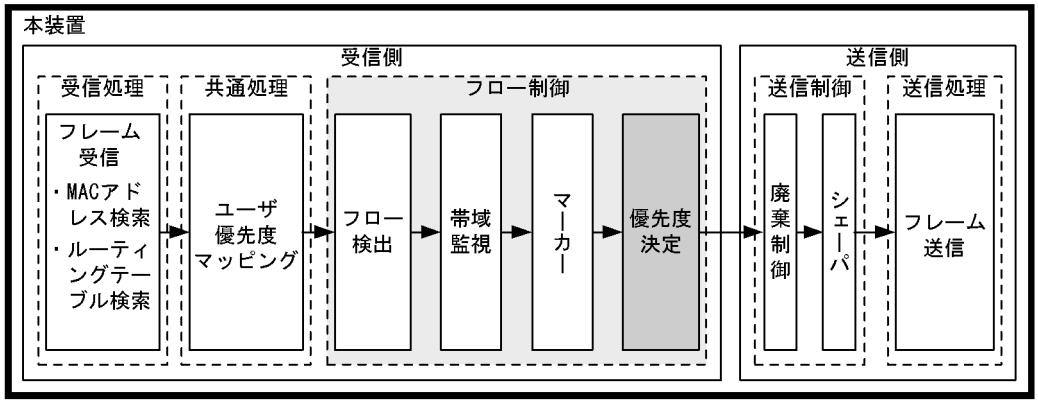
QOS-LIST3 のリスト情報に「replace-dscp 63」が表示されることを確認します。

3.10 優先度決定の解説

優先度決定は，フロー検出で検出したフレームの優先度を CoS 値で指定して，送信キューを決定する機能です。

この節で説明する優先度決定の位置づけを次の図に示します。

図 3-17 優先度決定の位置づけ



（凡例）：この節で説明するブロック

3.10.1 CoS 値・キューイング優先度

CoS 値は，フレームの装置内における優先度を表すインデックスを示します。キューイング優先度は，キューイングする各キューに対して廃棄されやすさの度合いを示します。

CoS 値とキューイング優先度の指定範囲を次の表に示します。

表 3-13 CoS 値とキューイング優先度の指定範囲

項目	指定範囲
CoS 値	0 ～ 7
キューイング優先度	1 ～ 3

CoS 値の指定は，ユーザ優先度引き継ぎと同時に設定することはできません。

また，フロー制御の優先度決定およびユーザ優先度引き継ぎが設定されていない場合は，次の表に示すデフォルトの CoS 値とキューイング優先度を使用します。

表 3-14 デフォルトの CoS 値とキューイング優先度

項目	デフォルト値	対象となるフレーム
CoS 値	ユーザ優先度マッピングに従います	• フロー検出で検出しないフレーム • フロー検出で検出し，優先度決定（CoS 値の指定）およびマーカー（優先度引き継ぎ）を実施しないフレーム
キューイング優先度	3	• フロー検出で検出しないフレーム • フロー検出で検出し，優先度決定（キューイング優先度値の指定）を実施しないフレーム

なお，次に示すフレームは，フロー制御の優先度決定およびユーザ優先度引き継ぎの有無にかかわらず，固定的に CoS 値とキューイング優先度を決定します。

優先度決定およびユーザ優先度引き継ぎで変更できないフレームを次の表に示します。

表 3-15　優先度決定で変更できないフレーム一覧

フレーム種別	CoS 値	キューイング優先度
本装置が自発的に送信するフレーム	7	3
本装置が受信するフレームのうち次のフレーム • ARP フレーム • 回線テストに使用するフレーム	5	3
本装置が受信するフレームのうち次のフレーム • MAC アドレス学習の移動検出とみなしたフレーム	2	3

3.10.2　CoS マッピング機能

CoS マッピング機能は，ユーザ優先度マッピングで決定した CoS 値，またはフロー制御の優先度決定で指定した CoS 値に基づいて，送信キューを決定する機能です。

CoS 値と送信キューのマッピングを次の表に示します。

表 3-16　CoS 値と送信キューのマッピング

CoS 値	送信時のキュー番号	
	送信キュー長 32	送信キュー長 728
0	1	1
1	2	1
2	3	1
3	4	1
4	5	1
5	6	1
6	7	1
7	8	2

3.10.3　IP マルチキャストパケットフロー制御補助モード

IP マルチキャストパケットを含むフローに対して，フロー制御の優先度決定を実施する場合に使用するモードです。

初期導入時のデフォルト設定では，本装置は IP マルチキャストパケットを受信した場合，VLAN 内のポートに中継するとともに本装置宛てとしても受信します。

IP マルチキャストパケットフロー制御補助モードでは，本装置宛てとしては受信しないで，VLAN 内のポートに中継するだけです。

本モードを使用すると，本装置宛てとして受信する制御フレームに影響を与えないで，IP マルチキャストパケットを含むフローに対して優先度決定を実施できます。IP マルチキャストパケットを含むフローに対して優先度決定を実施する場合は，本モードを使用してください。

なお，IP マルチキャストパケットフロー制御補助モードは system ip-multicast-qos-assist コマンドで設

定します。

3.10.4 優先度決定使用時の注意事項

(1) フレームの優先度決定

「フレームの優先度を上げる」動作を指定すると，次に示すフレームが受信または送信できなくなることによって，通信が切断される場合があります。

- 本装置宛てのプロトコル制御フレーム
- 本装置が自発的に送信するフレーム

このような現象が発生した場合は,「フレームの優先度を下げる」動作を実施してください。

(2) IP マルチキャストパケットフロー制御補助モードと IGMP snooping/MLD snooping との共存

IP マルチキャストパケットフロー制御補助モードの動作時に IGMP snooping/MLD snooping を使用した場合の動作を次の表に示します。

表 3-17 IP マルチキャストパケットフロー制御補助モードの動作時に IGMP snooping/MLD snooping を使用した場合の動作について

IGMP snooping	MLD snooping	IP マルチキャストパケット受信時	
		IPv4 マルチキャストパケット	IPv6 マルチキャストパケット
設定なし	設定なし	中継だけする	中継だけする
設定あり	設定なし	IGMP snooping を実施※1	中継だけする
設定なし	設定あり	中継だけする	MLD snooping を実施※2
設定あり	設定あり	IGMP snooping を実施※1	MLD snooping を実施※2

注※ 1

IGMP snooping を設定していない VLAN は，IPv4 マルチキャストパケットを受信した場合，VLAN 内のポートに中継するとともに本装置宛てとしても受信します。

注※ 2

MLD snooping を設定していない VLAN は，IPv6 マルチキャストパケットを受信した場合，VLAN 内のポートに中継するとともに本装置宛てとしても受信します。

(3) IP マルチキャストパケットフロー制御補助モードと IEEE802.1X との共存時の動作

IP マルチキャストパケットフロー制御補助モードと IEEE802.1X を同時に使用して，IEEE802.1X の端末検出動作切り替えオプションを auto に設定した場合，次に示すパケットでの端末検出はしません。

- 宛先アドレスが IPv4 マルチキャストアドレスのパケット
- 宛先アドレスの範囲が ff0::/12 以外の IPv6 マルチキャストパケット
- MLD パケット

(4) IP マルチキャストパケットフロー制御補助モードと MAC 認証との共存時の動作

IP マルチキャストパケットフロー制御補助モードと MAC 認証を同時に使用した場合，次に示すパケットでの認証はしません。

- 宛先アドレスが IPv4 マルチキャストアドレスのパケット

- 宛先アドレスの範囲が ff0::/12 以外の IPv6 マルチキャストパケット
- MLD パケット

3.11 優先度決定コンフィグレーション

3.11.1 CoS 値の設定

特定のフローに対して CoS 値を設定します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，CoS 値を設定します。

[コマンドによる設定]

1. **(config)#ip qos-flow-list QOS-LIST1**
   IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)#qos ip any host 192.168.100.10 action cos 6**
   192.168.100.10 の IP アドレスを宛先とし，CoS 値＝ 6 の IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)#exit**
   IPv4 QoS フローリストモードから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 gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

5. **(config-if)#ip qos-flow-group QOS-LIST1 in**
   IPv4 QoS フローリスト（QOS-LIST1）を有効にします。

3.11.2 IP マルチキャストパケットフロー制御補助モードの設定

IP マルチキャストパケットフロー制御補助モードを設定します。

[設定のポイント]

IP マルチキャストパケットを含むフローに対して優先度決定を使用する場合に設定します。

[コマンドによる設定]

1. **(config)#system ip-multicast-qos-assist**
   IP マルチキャストパケットフロー制御補助モードを有効にします。

3.12 優先度のオペレーション

3.12.1 優先度の確認

回線にトラフィック（宛先 IP アドレスが 192.168.100.10 のフレーム）を注入している状態で，show qos queueing コマンドによってキューイングされているキュー番号を確認します。対象のイーサネットインタフェースは，ポート 0/2 です。

図 3-18 優先度の確認

```
> show qos queueing 0/2

Date 2007/03/01 13:00:00 UTC
NIF0/Port2 (outbound)
 Max_Queue=8, Rate_limit=100Mbit/s, Burst_size=32kbyte, Qmode=pq/tail_drop
  Queue1: Qlen=  0, Limit_Qlen= 32
  Queue2: Qlen=  0, Limit_Qlen= 32
  Queue3: Qlen=  0, Limit_Qlen= 32
  Queue4: Qlen=  0, Limit_Qlen= 32
  Queue5: Qlen=  0, Limit_Qlen= 32
  Queue6: Qlen=  1, Limit_Qlen= 32                                  … 1
  Queue7: Qlen=  0, Limit_Qlen= 32
  Queue8: Qlen=  0, Limit_Qlen= 32
   discard packets
    HOL1=        0, HOL2=        0, Tail_drop=          0
```

1. Queue6 の Qlen の値がカウントされていることを確認します。

4 送信制御

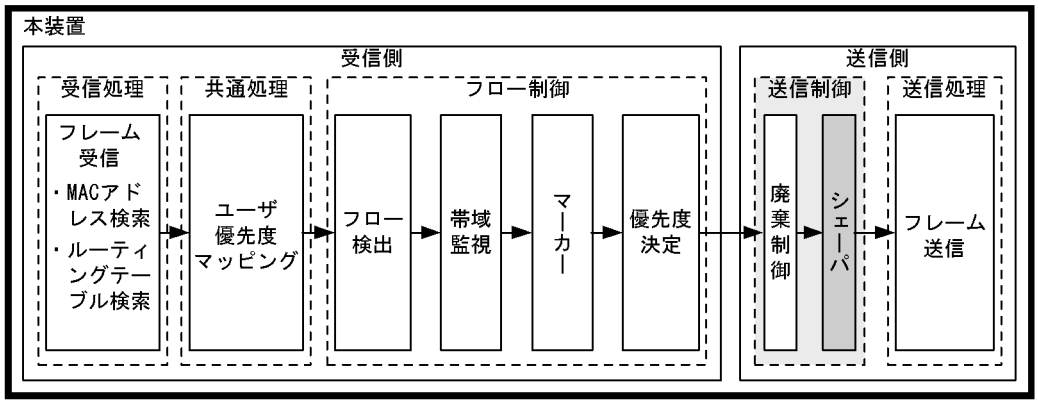
この章では本装置の送信制御（シェーパおよび廃棄制御）について説明します。

4.1 シェーパ解説

4.1.1 レガシーシェーパの概要

シェーパは，各キューからのフレームの出力順序，および各ポートの出力順序や出力帯域を制御する機能です。この節で説明するシェーパの位置づけを次の図に示します。

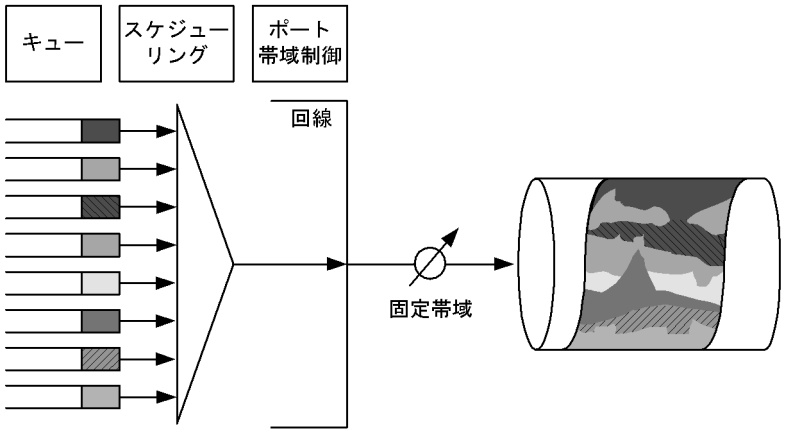
図 4-1 シェーパの位置づけ



（凡例）：この節で説明するブロック

レガシーシェーパは，次の図に示すように，どのキューにあるフレームを次に送信するかを決めるスケジューリングと，イーサネットインタフェースの帯域をシェーピングするポート帯域制御から構成されています。レガシーシェーパの概念を次の図に示します。

図 4-2 レガシーシェーパの概念



（凡例）：固定的に帯域をシェーピング

4.1.2 送信キュー長指定

本装置では，ネットワーク構成や運用形態に合わせて送信キュー長を変更できます。送信キュー長の変更はコンフィグレーションコマンド limit-queue-length で指定します。送信キュー長を拡大することによって，バーストトラフィックによるキューあふれを低減させることができます。なお，指定した送信キュー

長は本装置のすべてのイーサネットインタフェースに対して有効になります。

送信キュー長を指定しない場合，キュー長 32 で動作します。なお，キュー長 728 を指定する場合は，コンフィグレーションコマンド flowcontrol を使用して「ポーズパケットを送信する」設定をしてください。

表 4-1　送信キュー長と運用目的の関係

送信キュー長	運用目的
32	各キューに均等に負荷があり，送信制御を有効にしたい場合に指定します。
728※	バーストトラフィックによるキューあふれを低減させたい場合に指定します。

注※

送信キュー長 728 を指定した場合，キュー 1，キュー 2 に対してだけキュー長を割り当て動作するため，各スケジューリングの動作は次のようになります。

PQ，RR，WRR ：キュー 1，キュー 2 が PQ，RR，WRR で動作します。

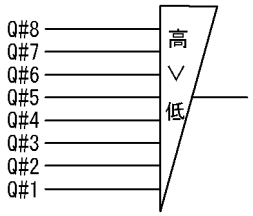
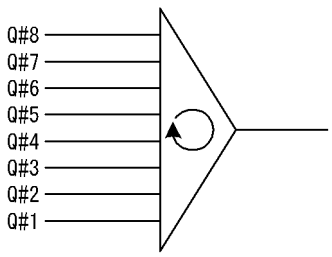
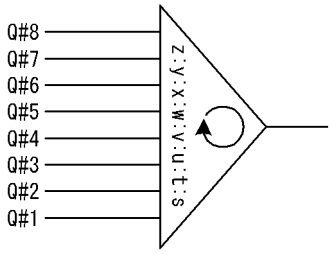
2PQ+6DRR　　：キュー 1，キュー 2 が DRR で動作します。

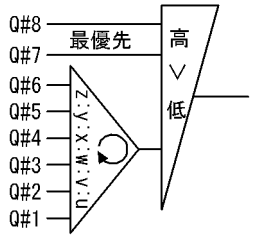
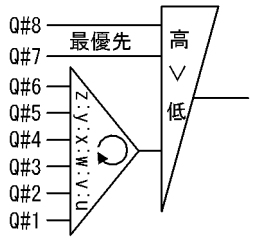
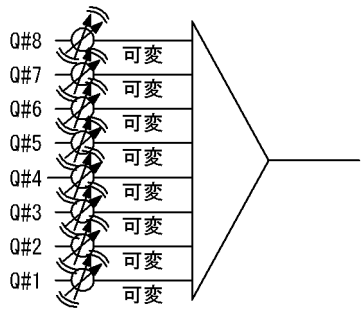
2PQ+6WRR　　：キュー 1，キュー 2 が WRR で動作します。

4.1.3　スケジューリング

スケジューリングは，各キューに積まれたフレームをどのような順序で送信するかを制御する機能です。本装置では，次に示す六つのスケジューリング機能があります。スケジューリングの動作説明を次の表に示します。

表 4-2　スケジューリングの動作説明

スケジューリング種別	概念図	動作説明	適用例
PQ		完全優先制御。複数のキューにフレームがキューイングされている場合，優先度の高いキューから常にフレームを送出します。	トラフィック優先順を完全に遵守する場合
RR		ラウンドロビン。複数のキューにフレームが存在する場合，順番にキューを見ながら１フレームずつ送出します。フレーム長によらず，フレーム数が均等になる制御を行います。	データ系トラフィックだけの場合
WRR		重み（フレーム数）付きラウンドロビン。複数のキューにフレームが存在する場合，順番にキューを見ながら設定した z：y：x：w：v：u：t：s の重み（フレーム数）に応じて，キュー８～１（左図 Q#8 ～ Q#1）からフレームを送出します。	すべてのトラフィックの送信が要求されかつ，優先すべきトラフィックと優先しないトラフィックが混在している場合

スケジューリング種別	概念図	動作説明	適用例
2PQ+6DRR		最優先キュー＋重み（バイト数）付きラウンドロビン。最優先のキュー 8（左図 Q#8）は，常に最優先でフレームを送出します。キュー 7（左図 Q#7）は，キュー 8（左図 Q#8）の次に優先的にフレームを送出します。キュー 8,7 の送出がないときに，キュー 6 ～ 1（左図 Q#6 ～ Q#1）は各キュー設定したバイト数（z：y：x：w：v：u）に応じてフレームを送出します。	最優先キューに映像，音声，DRR キューにデータ系トラフィック
2PQ+6WRR		最優先キューと重み（フレーム数）付きラウンドロビン。最優先のキュー 8（左図 Q#8）は，常に最優先でフレームを送出します。キュー 7（左図 Q#7）は，キュー 8（左図 Q#8）の次に優先的にフレームを送出します。キュー 8,7 の送出がないときに，キュー 6 ～ 1（左図 Q#6 ～ Q#1）は各キュー設定したフレームの重み（z：y：x：w：v：u）に応じてフレームを送出します。	最優先キューに映像，音声，WRR キューにデータ系トラフィック
WFQ		重み付き均等保証。すべてのキューに対して重み（最低保証帯域）を設定し，はじめにキューごとに最低保証帯域分を送出します。	すべてのトラフィックに対し最低帯域保証が要求される場合

スケジューリングの仕様について次の表に示します。

表 4-3　スケジューリング仕様

項目		仕様
キュー数		8 キュー
2PQ+6DRR	キュー 1 ～ 6 の重みの設定範囲	【kbyte 単位】 10，20，40，80，160，320，640，1280，2560，5120，10000，20000，40000，80000，160000 【Mbyte 単位】 10M，20M，40M，80M，160M
2PQ+6WRR	キュー 1 ～ 6 の重みの設定範囲	1 ～ 15
WFQ	キュー 1 ～ 8 の重みの設定範囲	「表 4-4　WFQ の設定範囲」を参照してください。最低保証帯域の合計が回線帯域以下になるように設定してください。回線状態が半二重モードの場合は設定できません。設定できない場合は，運用ログが表示され WFQ の設定は無効となり，PQ で動作します。

項目		仕様
	最低保証帯域の対象となるフレームの範囲	MAC ヘッダから FCS まで

表 4-4 WFQ の設定範囲

設定単位※1	設定範囲	刻み値
Gbit/s	1G ～ 10G	1Gbit/s
Mbit/s	1M ～ 10000M	1Mbit/s
kbit/s	1000 ～ 10000000	100kbit/s※2
	64 ～ 960	64kbit/s※3

注※1 1G，1M，1k はそれぞれ 1000000000，1000000，1000 として扱います。
注※2 設定値が 1000k 以上の場合 100k 刻みで指定します（1000，1100，1200，…，10000000）。
注※3 設定値が 1000k 未満の場合 64k 刻みで指定します（64，128，192，…，960）。

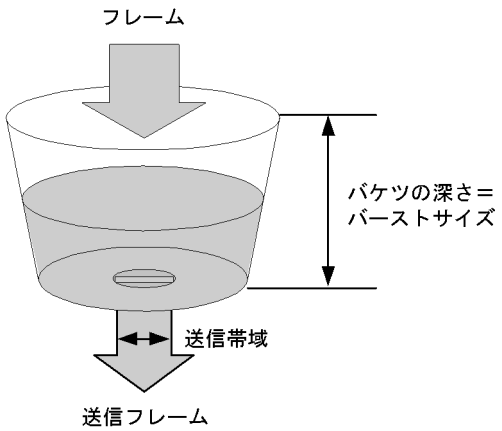
4.1.4 ポート帯域制御

ポート帯域制御は，スケジューリングを実施した後に，該当するポートに指定した送信帯域にシェーピングする機能です。この制御を使用して，広域イーサネットサービスへ接続できます。

例えば，回線帯域が 1Gbit/s で ISP との契約帯域が 400Mbit/s の場合，ポート帯域制御機能を使用してあらかじめ帯域を 400Mbit/s 以下に抑えてフレームを送信することができます。

ポート帯域制御は穴の開いたバケツをモデルとする，Leaky Bucket アルゴリズムを用いています。Leaky Bucket アルゴリズムのモデルを次の図に示します。

図 4-3 Leaky Bucket アルゴリズムのモデル



バケツには受信したフレームサイズ分の水が注ぎ込まれ，ポート帯域制御の送信帯域分の水が送信フレームとして流れます。水が一時的に大量に注ぎこまれたときに許容できる量，すなわちバケツの深さがバーストサイズに対応します。バケツが空の状態でトラフィックを送信した際，送信帯域の揺らぎはバーストサイズに比例します。バーストサイズまで水が溜まった場合，フレームは送信キューに溜まります。

ポート帯域制御の設定範囲を次の表に示します。設定帯域は回線速度以下になるように設定してください。

回線状態が半二重モードの場合は設定できません。設定できない場合，運用ログが表示されポート帯域制御の設定は無効となります。

表 4-5 ポート帯域制御の設定範囲

設定単位※1	設定範囲	刻み値
Gbit/s	1G ～ 10G	1Gbit/s
Mbit/s	1M ～ 10000M	1Mbit/s
kbit/s	1000 ～ 10000000	100kbit/s※2
	64 ～ 960	64kbit/s※3

注※1 1G，1M，1k はそれぞれ 1000000000，1000000，1000 として扱います。
注※2 設定値が 1000k 以上の場合 100k 刻みで指定します（1000，1100，1200，…，10000000）。
注※3 設定値が 1000k 未満の場合 64k 刻みで指定します（64，128，192，…，960）。

バーストサイズの設定範囲を次に示します。

● バーストサイズの設定範囲

4，8，16，32kbyte（設定省略時のデフォルトは 32kbyte）

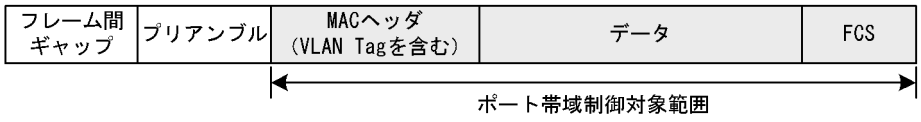
Leaky Bucket アルゴリズムの特性によるバーストサイズの特徴を次の表に示します。

表 4-6 バーストサイズの特徴

バーストサイズ	特徴
小さくする	バーストトラフィックが比較的廃棄されやすい。通信をしていない状態でトラフィックを送信した際，送信帯域の揺らぎが比較的小さい。
大きくする	バーストトラフィックが比較的廃棄されにくい。通信をしていない状態でトラフィックを送信した際，送信帯域の揺らぎが比較的大きい。

ポート帯域制御の対象となるフレームの範囲は MAC ヘッダから FCS までです。ポート帯域制御の対象範囲を次の図に示します。

図 4-4 ポート帯域制御の対象範囲



4.1.5 シェーパ使用時の注意事項

(1) パケットバッファ枯渇時のスケジューリングの注意事項

出力回線の帯域を上回るトラフィックを受信したとき，本装置のパケットバッファの枯渇が発生する場合があります。そのため，受信したフレームがキューにキューイングされず廃棄されるため，指定したスケジューリングどおりにフレームが送信されない場合があります。

パケットバッファの枯渇については，show qos queueing コマンドの HOL1 または HOL2 カウンタがインクリメントされていることで確認できます。

パケットバッファの枯渇が定常的に発生する場合，ネットワーク設計の見直しが必要です。

4.2 シェーパのコンフィグレーション

4.2.1 スケジューリングの設定

[設定のポイント]

スケジューリングを設定したQoSキューリスト情報を作成し，該当するポートに設定します。

[コマンドによる設定]

1. **(config)#qos-queue-list QLIST-PQ pq**
   QoSキューリスト情報（QLIST-PQ）にスケジューリング（PQ）を設定します。

2. **(config)#interface gigabitethernet 0/1**
   ポート0/1のインタフェースモードに移行します。

3. **(config-if)#qos-queue-group QLIST-PQ**
   QoSキューインタフェース情報にQoSキューリスト名称を指定し，QoSキューリスト情報を有効にします。

4.2.2 ポート帯域制御の設定

該当するポートの出力帯域を実回線の帯域より低くする場合に設定します。

[設定のポイント]

該当するポート（100Mbit/s）に対し，ポート帯域制御による帯域の設定（20Mbit/s）およびバーストサイズの設定（4kbyte）を行います。

[コマンドによる設定]

1. **(config)#interface gigabitethernet 0/13**
   ポート0/13のインタフェースモードに移行します。

2. **(config-if)#speed 100**
   (config-if)#duplex full
   該当するポートの回線速度を100Mbit/sに設定します。

3. **(config-if)#traffic-shape rate 20M 4**
   ポート帯域を20Mbit/s，バーストサイズを4kbyteに設定します。

4.3 シェーパのオペレーション

show qos queueing コマンドによって，イーサネットインタフェースに設定したレガシーシェーパの内容を確認します。

4.3.1 スケジューリングの確認

スケジューリングの確認方法を次の図に示します。

図 4-5 スケジューリングの確認

```
> show qos queueing 0/1

Date 2007/03/01 13:00:00 UTC
NIF0/Port1 (outbound)
 Max_Queue=8, Rate_limit=100Mbit/s, Burst_size=32kbyte, Qmode=pq/tail_drop …1
  Queue1: Qlen=  0, Limit_Qlen= 32
  Queue2: Qlen=  0, Limit_Qlen= 32
  Queue3: Qlen=  0, Limit_Qlen= 32
  Queue4: Qlen=  0, Limit_Qlen= 32
  Queue5: Qlen=  0, Limit_Qlen= 32
  Queue6: Qlen=  0, Limit_Qlen= 32
  Queue7: Qlen=  0, Limit_Qlen= 32
  Queue8: Qlen=  0, Limit_Qlen= 32
   discard packets
    HOL1=        0, HOL2=        0, Tail_drop=          0
```

1. Qmode パラメータの内容が，設定したスケジューリング（この例では，pq/tail_drop）になっていることを確認します。

4.3.2 ポート帯域制御の確認

ポート帯域制御の確認方法を次の図に示します。

図 4-6 ポート帯域制御の確認

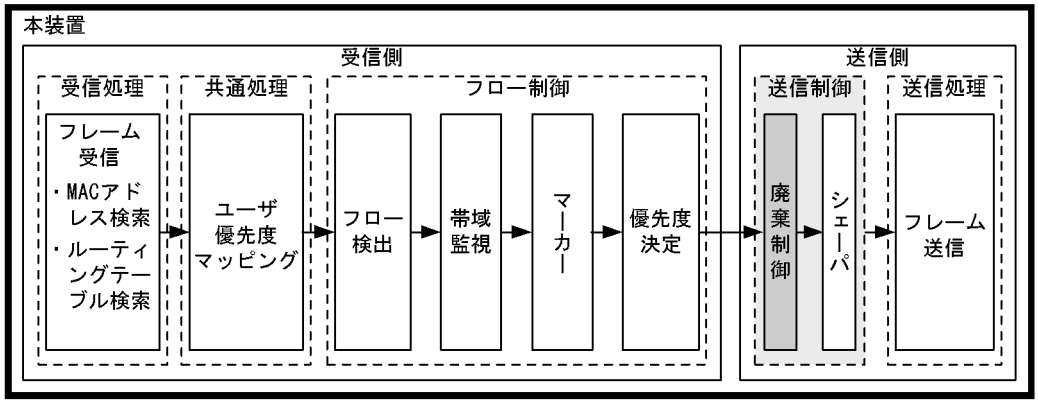
```
> show qos queueing 0/13

Date 2007/03/01 13:00:00 UTC
NIF0/Port13 (outbound)
 Max_Queue=8, Rate_limit=20Mbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop … 1,2
  Queue1: Qlen=  0, Limit_Qlen= 32
  Queue2: Qlen=  0, Limit_Qlen= 32
  Queue3: Qlen=  0, Limit_Qlen= 32
  Queue4: Qlen=  0, Limit_Qlen= 32
  Queue5: Qlen=  0, Limit_Qlen= 32
  Queue6: Qlen=  0, Limit_Qlen= 32
  Queue7: Qlen=  0, Limit_Qlen= 32
  Queue8: Qlen=  0, Limit_Qlen= 32
   discard packets
    HOL1=        0, HOL2=        0, Tail_drop=          0
```

1. Rate_limit パラメータの内容が，指定した帯域値（この例では，20Mbit/s）になっていることを確認します。
2. Burst_size パラメータの内容が，指定したバーストサイズ（この例では，4kbyte）になっていることを確認します。

4.4 廃棄制御解説

この節で説明する廃棄制御の位置づけを次の図に示します。

図 4-7 廃棄制御の位置づけ



（凡例）：この節で説明するブロック

4.4.1 廃棄制御

廃棄制御は，キューイングする各キューに対して廃棄されやすさの度合いを示すキューイング優先度と，キューにフレームが滞留している量に応じて，該当フレームをキューイングするか廃棄するかを制御する機能です。

キューにフレームが滞留している場合，キューイング優先度を変えることによって，さらに木目細かいQoSを実現できます。

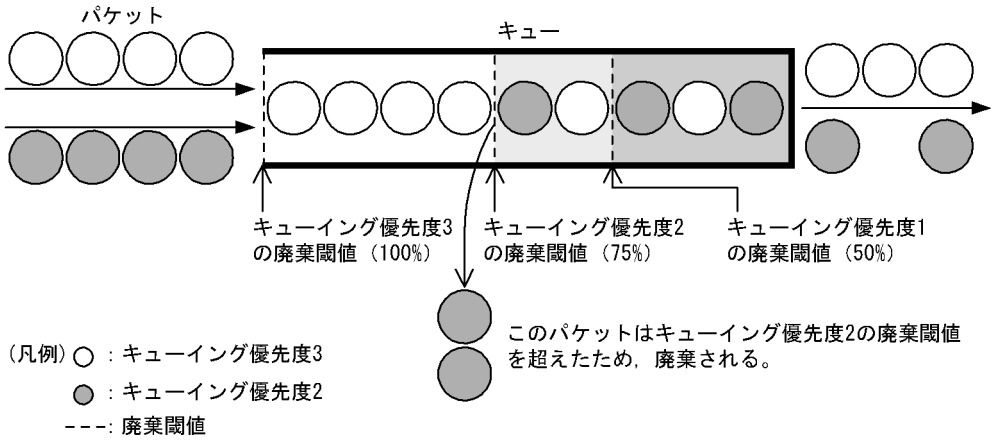
一つのキューにキューイングできるフレーム数を「キュー長」と呼びます。

本装置は，テールドロップ方式で廃棄制御を行います。

(1) テールドロップ

キュー長が廃棄閾値を超えると，フレームを廃棄する機能です。廃棄閾値は，キューイング優先度ごとに異なり，キューイング優先度値が高いほどフレームが廃棄されにくくなります。テールドロップの概念を次の図に示します。キューイング優先度2の廃棄閾値を超えると，キューイング優先度2のフレームをすべて廃棄します。

図 4-8　テールドロップの概念



次に，テールドロップ機能におけるキューイング優先度ごとの廃棄閾値を次の表に示します。廃棄閾値は，キュー長に対するキューの溜まり具合を百分率で表します。

表 4-7　テールドロップでの廃棄閾値

キューイング優先度	廃棄閾値［%］
1	50
2	75
3	100

4.5 廃棄制御のコンフィグレーション

4.5.1 キューイング優先度の設定

特定のフローに対してキューイング優先度を設定します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出を行い，キューイング優先度を設定します。

[コマンドによる設定]

1. **(config)#ip qos-flow-list QOS-LIST2**
   IPv4 QoS フローリスト（QOS-LIST2）を作成します。本リストを作成することによって，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)#qos ip any host 192.168.100.10 action discard-class 2**
   192.168.100.10 の IP アドレスを宛先とし，キューイング優先度＝ 2 の QoS フローリストを設定します。

3. **(config-ip-qos)#exit**
   IPv4 QoS フローリストモードから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 gigabitethernet 0/1**
   ポート 0/1 のインタフェースモードに移行します。

5. **(config-if)#ip qos-flow-group QOS-LIST2 in**
   受信側に QoS フローリスト（QOS-LIST2）を有効にします。

4.6 廃棄制御のオペレーション

回線にトラフィック（Queue6 の Qlen が 32 程度の滞留が発生するトラフィック）を注入している状態で，show qos queueing コマンドによってキューイングされているキュー番号および廃棄パケット数を確認します。対象のイーサネットインタフェースは，ポート 0/2 です。

4.6.1 キューイング優先度の確認

キューイング優先度の確認方法を次の図に示します。

図 4-9 キューイング優先度の確認

```
> show qos queueing 0/2

Date 2007/03/01 13:00:00 UTC
NIF0/Port2 (outbound)
 Max_Queue=8, Rate_limit=100Mbit/s, Burst_size=32kbyte, Qmode=pq/tail_drop
  Queue1: Qlen=  0, Limit_Qlen= 32
  Queue2: Qlen=  0, Limit_Qlen= 32
  Queue3: Qlen=  0, Limit_Qlen= 32
  Queue4: Qlen=  0, Limit_Qlen= 32
  Queue5: Qlen=  0, Limit_Qlen= 32
  Queue6: Qlen= 24, Limit_Qlen= 32                                  … 1,2
  Queue7: Qlen=  0, Limit_Qlen= 32
  Queue8: Qlen=  0, Limit_Qlen= 32
   discard packets
    HOL1=    1514, HOL2=       0, Tail_drop=         18            … 2
```

1. Queue6 の Qlen の値がカウントされていることを確認します。
2. Qlen の値が Limit_Qlen の値の 75% であり，discard packets の Tail_drop のカウンタがインクリメントされていることを確認します。

5 レイヤ 2 認証

この章では，本装置のレイヤ 2 認証機能の概要について説明します。

5.1 概要

5.1.1 レイヤ 2 認証種別

本装置には，次に示すレイヤ 2 レベルの認証機能があります。

- IEEE802.1X
  IEEE802.1X に準拠したユーザ認証をする機能です。IEEE802.1X 認証に必要な EAPOL パケットを送信する端末を認証します。
- Web 認証
  Web 認証は，汎用 Web ブラウザを利用してユーザ認証をする機能です。汎用 Web ブラウザを使用できる端末で認証操作をします。
- MAC 認証
  MAC 認証は，プリンタなど，ユーザによる認証操作ができない端末を認証する機能です。
- 認証 VLAN【OP-VAA】
  認証 VLAN は，専用の認証サーバと連携してユーザ認証をする機能です。

レイヤ 2 認証には，認証動作による認証モードがあります。認証モードごとの機能概要を次の表に示します。

また，これらの機能は，組み合わせて利用できる機能と利用できない機能があります。機能の組み合わせについては「5.2　レイヤ 2 認証と他機能との共存について」を参照してください。

表 5-1　レイヤ 2 認証でサポートする機能

レイヤ 2 認証	認証モード	概要
IEEE802.1X	ポート単位認証	物理ポートまたはチャネルグループに対して認証を制御します。一つの物理ポートまたは一つのチャネルグループが一つの認証単位となります。また，ポート単位認証には次に示す三つの認証サブモードがあり，それぞれ認証動作が異なります。 1. シングルモード 一つの認証単位に一つの端末だけ認証して接続します。最初に認証した端末以外の端末から認証要求があると，そのポートの認証状態は未認証状態に戻ります。 2. マルチモード 一つの認証単位に複数端末の接続を許容します。最初に認証した端末以外の端末は認証しません。 3. 端末認証モード 一つの認証単位に複数端末の接続を許容し，端末ごとに認証を行います。
	VLAN 単位認証（静的）	VLAN に対して認証を制御します。複数の端末が接続できます。端末ごとに認証を行い，認証に成功すると VLAN 内で通信できます。
	VLAN 単位認証（動的）	MAC VLAN に所属する端末に対して認証を制御します。複数の端末が接続できます。認証に成功すると MAC VLAN で切り替えた VLAN で通信できます。
Web 認証	固定 VLAN モード	ユーザ認証成功後は，VLAN 内へ通信できます。
	ダイナミック VLAN モード	ユーザ認証成功後は，MAC VLAN で切り替えた VLAN 内へ通信できます。MAC VLAN が設定された物理ポートに認証を設定します。
	レガシーモード	ユーザ認証成功後は，MAC VLAN で切り替えた VLAN 内へ通信できます。MAC VLAN の VLAN に認証を設定します。
MAC 認証	固定 VLAN モード	認証成功後は，VLAN 内へ通信できます。

レイヤ 2 認証	認証モード	概要
	ダイナミック VLAN モード	認証成功後は，MAC VLAN で切り替えた VLAN 内へ通信できます。
認証 VLAN	―	認証 VLAN 専用サーバで認証を行い，認証結果によって本装置の MAC VLAN で VLAN を切り替えます。切り替え後の VLAN 内へ通信できます。

（凡例） ―：該当しない

5.1.2 認証方式

レイヤ 2 認証には装置内蔵の認証データで認証するローカル認証方式と，RADIUS サーバで認証する RADIUS 認証方式があります。認証 VLAN を除くレイヤ 2 認証に対応する認証方式を次の表に示します。

表 5-2 レイヤ 2 認証の認証方式

レイヤ 2 認証	認証モード	ローカル認証方式	RADIUS 認証方式
IEEE802.1X	ポート単位認証	×	○
	VLAN 単位認証（静的）	×	○
	VLAN 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	○	○
	レガシーモード	○	○
MAC 認証	固定 VLAN モード	○	○
	ダイナミック VLAN モード	○	○

（凡例） ○：対応する ×：対応しない

5.1.3 MAC VLAN の動的 VLAN 設定とレイヤ 2 認証

次の表に示すレイヤ 2 認証と認証モードで，MAC VLAN の認証対象ポートに認証済み端末を収容する認証後 VLAN を動的に設定します。また，接続されている認証対象ポートから認証対象端末がすべて認証解除された場合，動的に設定されていた VLAN は削除されます。

表 5-3 動的に VLAN が設定できるレイヤ 2 認証機能と認証モード

レイヤ 2 認証機能	認証モード
IEEE802.1X	VLAN 単位認証（動的）
Web 認証	ダイナミック VLAN モード
MAC 認証	ダイナミック VLAN モード

なお，コンフィグレーションコマンド switchport mac vlan が設定されている認証対象の MAC ポートでは，コンフィグレーションコマンドで設定された認証後 VLAN 以外の VLAN 切り替えはできません。さらに，認証対象の MAC ポートに動的に VLAN が設定されている状態で，コンフィグレーションコマンド switchport mac vlan が設定された場合，該当ポートに動的に設定された VLAN を認証後 VLAN とした認証端末はすべて認証が解除されます。

5.2 レイヤ 2 認証と他機能との共存について

レイヤ 2 認証と他機能との共存について説明します。

5.2.1 レイヤ 2 認証と他機能との共存

レイヤ 2 認証と他機能との共存仕様を次の表に示します。

表 5-4 他機能との共存仕様

レイヤ 2 認証機能	機能名		共存仕様
IEEE802.1X	リンクアグリゲーション		LACP リンクアグリゲーションのチャネルグループと同時に設定しないでください。
	VLAN	ポート VLAN	ポート単位認証および VLAN 単位認証（静的）で使用できます。
		プロトコル VLAN	装置で同時に使用できません。
		MAC VLAN	VLAN 単位認証（動的）で使用できます。
	デフォルト VLAN		ポート単位認証および VLAN 単位認証（静的）で使用できます。 VLAN 単位認証（動的）では認証前 VLAN に使用できます。
	VLAN 拡張機能	VLAN トンネリング	装置で同時に使用できません。
		EAPOL フォワーディング	装置で同時に使用できません。
	スパニングツリー		スパニングツリーを設定したポートには，ポート単位認証または VLAN 単位認証（静的）を設定しないでください。
	Ring Protocol		Ring Protocol を設定したリングポートには，ポート単位認証または VLAN 単位認証（静的）を設定しないでください。
	IGMP snooping		ポート単位認証または VLAN 単位認証（静的）と同時に設定しないでください。
	認証 VLAN		装置で同時に使用できません。
	GSRP		装置で同時に使用できません。
	アップリンク・リダンダント		アップリンクポートで使用できません。
	IEEE802.3ah/UDLD		ポート単位認証または VLAN 単位認証（静的）で設定されたポートでは使用しないでください。
	OADP，CDP		透過できません。
Web 認証	リンクアグリゲーション		固定 VLAN モードおよびダイナミック VLAN モードの認証ポートとして，チャネルグループのポートは使用できません。
	VLAN	ポート VLAN	固定 VLAN モードで使用できます。
		プロトコル VLAN	装置で同時に使用できません。
		MAC VLAN	ダイナミック VLAN モードおよびレガシーモードで使用できます。

レイヤ 2 認証機能	機能名		共存仕様
	デフォルト VLAN		固定 VLAN モードで使用できます。 ダイナミック VLAN モードおよびレガシーモードでは認証前 VLAN に使用できます。
	VLAN 拡張機能	VLAN トンネリング	装置で同時に使用できません。
		EAPOL フォワーディング	共存できます。
	スパニングツリー		スパニングツリーを設定したポートには，固定 VLAN モードまたはダイナミック VLAN モードを設定しないでください。
	Ring Protocol		Ring Protocol を設定したリングポートには，固定 VLAN モードまたはダイナミック VLAN モードを設定しないでください。
	IGMP snooping ※		装置で同時に使用できません。
	認証 VLAN		装置で同時に使用できません。
	DHCP snooping		レガシーモードで指定された VLAN ID が設定されたポートでは使用できません。
	アップリンク・リダンダント		アップリンクポートで使用できません。
	IEEE802.3ah/UDLD		固定 VLAN モードまたはダイナミック VLAN モードを設定したポートでは使用しないでください。
MAC 認証	リンクアグリゲーション		固定 VLAN モードおよびダイナミック VLAN モードの認証ポートとして，チャネルグループのポートは使用できません。
	VLAN	ポート VLAN	固定 VLAN モードで使用できます。
		プロトコル VLAN	装置で同時に使用できません。
		MAC VLAN	ダイナミック VLAN モードで使用できます。
	デフォルト VLAN		固定 VLAN モードで使用できます。 ダイナミック VLAN モードでは認証前 VLAN に使用できます。
	VLAN 拡張機能	VLAN トンネリング	装置で同時に使用できません。
		EAPOL フォワーディング	共存できます。
	スパニングツリー		スパニングツリーを設定したポートには，MAC 認証を設定しないでください。
	Ring Protocol		Ring Protocol を設定したリングポートには，MAC 認証を設定しないでください。
	IGMP snooping		装置で同時に使用できません。
	認証 VLAN		装置で同時に使用できません。
	アップリンク・リダンダント		アップリンクポートで使用できません。
	IEEE802.3ah/UDLD		MAC 認証を設定したポートでは使用しないでください。
認証 VLAN	VLAN	ポート VLAN	認証 VLAN の認証端末は接続できません。
		プロトコル VLAN	装置で同時に使用できません。
		MAC VLAN	認証 VLAN の認証端末を接続します。

レイヤ 2 認証機能	機能名		共存仕様
	デフォルト VLAN		認証前 VLAN に使用できます。
	VLAN 拡張機能	VLAN トンネリング	装置で同時に使用できません。
		EAPOL フォワーディング	装置で同時に使用できません。
	IEEE802.1X Web 認証 MAC 認証		装置で同時に使用できません。

注※　Web 認証のレガシーモードは，IGMP snooping と共存できます。

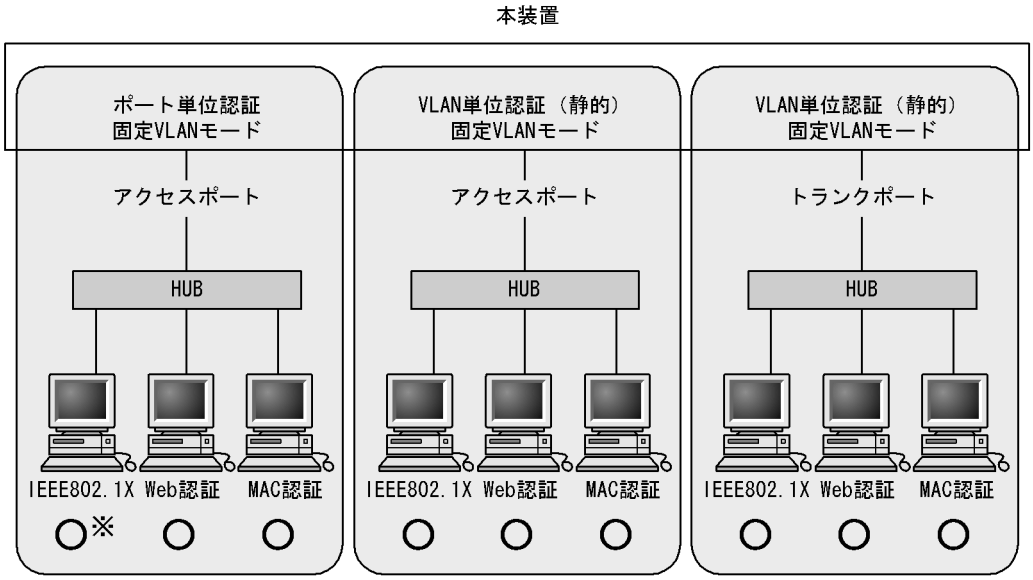
5.2.2 同一ポート内での共存

同一ポートに各レイヤ 2 認証の対象ポートとして設定された場合，どの認証モードの組み合わせであれば動作するかを次に示します。

- 固定 VLAN モードの共存
- ダイナミック VLAN モードの共存
- 固定 VLAN モードとダイナミック VLAN モードの共存
- レガシーモードの共存

(1) 同一ポートの固定 VLAN モードの共存

図 5-1 同一ポートの固定 VLAN モードの共存



（凡例）○：動作できる

注※ Web認証およびMAC認証を設定したポートにIEEE802.1Xポート単位認証を設定した場合は，端末認証モードを設定してください。
シングルモードおよびマルチモードを設定しないでください。
［設定しないコンフィグレーションコマンド］

```
dot1x force-authorized-port
dot1x port-control force-authorized
dot1x port-control force-unauthorized
dot1x multiple-hosts
```

表 5-5 同一ポートの固定 VLAN モードの共存

ポートの種類	IEEE802.1X		Web 認証（固定 VLAN モード）	MAC 認証（固定 VLAN モード）
	ポート単位認証	VLAN 単位認証（静的）		
アクセスポート	○※1	－	○	○
	－	○	○	○
チャネルグループのポート（アクセスポート）	○	×	－	－
	－	○	－	－
トランクポート	－	○※2	○	○
チャネルグループのポート（トランクポート）	－	○※2	－	－
上記以外	－	－	－	－

（凡例）
○：動作できる
×：コンフィグレーションで設定できるが動作できない

－：コンフィグレーションで設定できない

注※ 1

Web 認証および MAC 認証を設定したポートに IEEE802.1X のポート単位認証を設定した場合は，端末認証モードを設定してください。シングルモードおよびマルチモードを設定しないでください。

［設定しないコンフィグレーションコマンド］

dot1x force-authorized-port

dot1x port-control force-authorized

dot1x port-control force-unauthorized

dot1x multiple-hosts

注※ 2

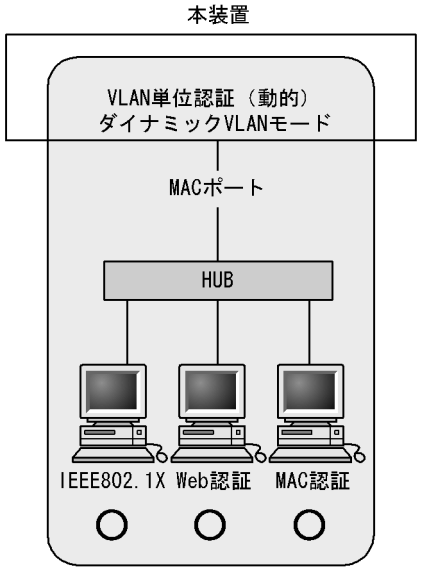
認証対象の VLAN と認証対象外の VLAN を同一ポートに設定した場合，認証対象外の VLAN では通信できません。ただし，認証除外ポートオプションを設定している場合は通信できます。

［表の見方の一例］

接続先がアクセスポートの場合，IEEE802.1X のポート単位認証，Web 認証（固定 VLAN モード），MAC 認証（固定 VLAN モード）の三つの認証モードを同一ポートで利用できます。または，IEEE802.1X の VLAN 単位認証（静的），Web 認証（固定 VLAN モード），MAC 認証（固定 VLAN モード）の三つの認証モードを同一ポートで利用できます。

(2) 同一ポートのダイナミック VLAN モードの共存

図 5-2 同一ポートのダイナミック VLAN モードの共存



（凡例）○：動作できる

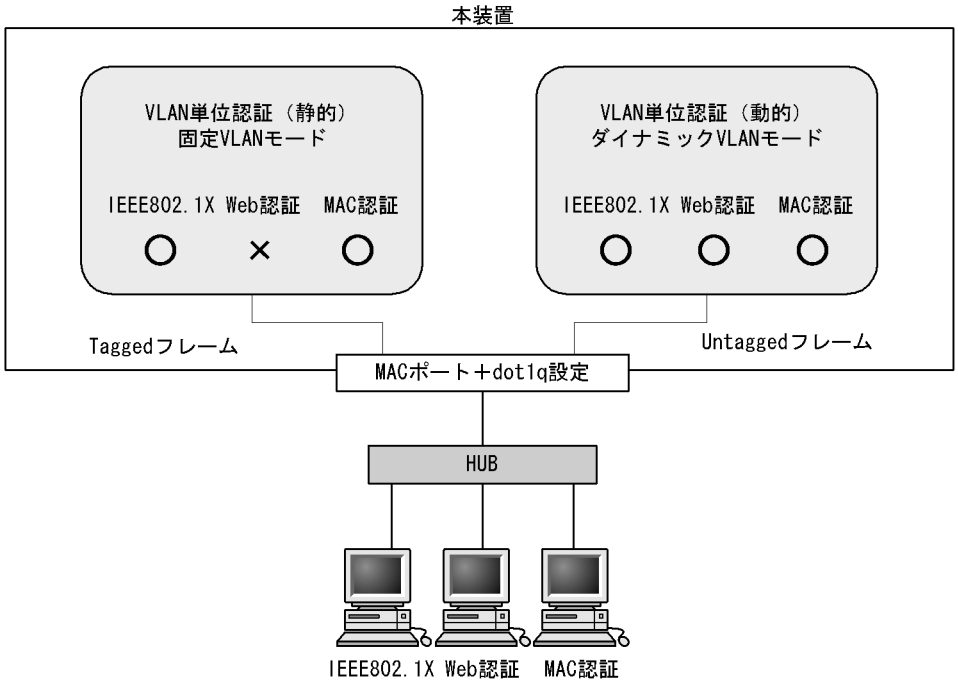
表 5-6 同一ポートのダイナミック VLAN モードの共存

ポートの種類	IEEE802.1X VLAN 単位認証（動的）	Web 認証（ダイナミック VLAN モード）	MAC 認証（ダイナミック VLAN モード）
MAC ポート	○	○	○
上記以外	×	×	×

（凡例） ○：動作できる ×：動作できない

(3) 同一ポートのダイナミック VLAN モードと固定 VLAN モードの共存

図 5-3 同一ポートのダイナミック VLAN モードと固定 VLAN モードの共存



（凡例）○：動作できる　×：動作できない

表 5-7 同一ポートのダイナミック VLAN モードと固定 VLAN モードの共存

ポートの種類	受信フレームの種類	IEEE802.1X		Web 認証		MAC 認証	
		VLAN 単位認証（静的）	VLAN 単位認証（動的）	固定 VLAN モード	ダイナミック VLAN モード	固定 VLAN モード	ダイナミック VLAN モード
MAC ポート＋ dot1q 設定	Tagged フレーム	○※1	×	×	×	○	×
	Untagged フレーム	×	○	○※2	○	○※2	○

（凡例） ○：動作できる　×：動作できない

注※ 1

認証対象の VLAN と認証対象外の VLAN を同一ポートに設定した場合，認証対象外の VLAN では通信できません。ただし，認証除外ポートオプションを設定している場合は通信できます。

注※ 2

RADIUS 認証方式で，RADIUS サーバから認証後 VLAN が送られてこなかった場合，ネイティブ VLAN に収容して固定 VLAN と同様に扱います。ただし，ポート間の移動については，ダイナミック VLAN モードの動作に従います。

(4) 同一ポートのレガシーモードの共存

表 5-8 同一ポートのレガシーモードの共存

ポートの種類	IEEE802.1X VLAN 単位認証（動的）	Web 認証（レガシーモード）	MAC 認証（全モード）
MAC ポート	○	○	×
上記以外	×	×	×

（凡例） ○：動作できる ×：動作できない

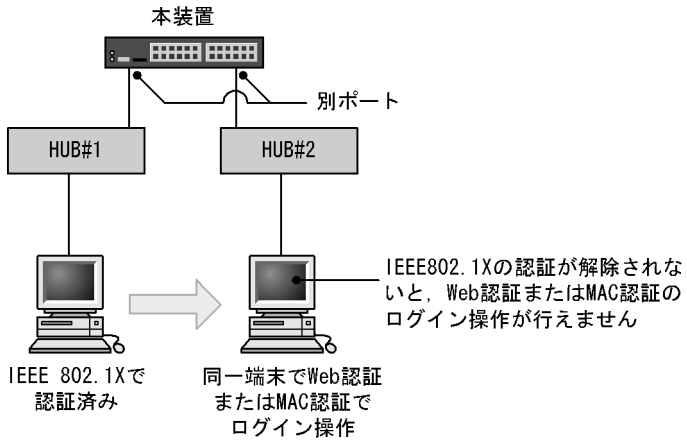
5.2.3 レイヤ 2 認証共存時の認証優先

(1) IEEE802.1X と Web 認証または MAC 認証との共存時の認証優先

同一端末（同一 MAC アドレスを持つ端末）で，Web 認証または MAC 認証による成功後に，IEEE802.1X のポート単位認証または VLAN 単位認証（静的）による認証に成功した場合，IEEE802.1X の認証結果が優先され，Web 認証または MAC 認証の認証状態は解除されます（Web 認証では，この場合ログアウト画面は表示されません）。

また，次に示す図のように別々のポートに接続された HUB（図では HUB#1）を介して接続されている端末が，すでに IEEE802.1X（ポート単位認証（端末認証モード）または VLAN 単位認証（静的））で認証されている状態で，別の HUB（図では HUB#2）に接続を変更した場合，いったん IEEE802.1X の認証が解除されないと Web 認証（固定 VLAN モード）または MAC 認証（固定 VLAN モード）のログイン操作を行うことはできません。IEEE802.1X の運用コマンド clear dot1x auth-state で認証を解除してください。

図 5-4 IEEE802.1X で認証されている端末のポート移動後の Web 認証または MAC 認証使用



また，同一端末で，Web 認証（ダイナミック VLAN モードまたはレガシーモード）または MAC 認証（ダイナミック VLAN モード）による認証成功後，IEEE802.1X の VLAN 単位認証（動的）による認証に成功した場合，IEEE802.1X の認証結果が優先されて IEEE802.1X で設定された VLAN に切り替わり，Web 認証または MAC 認証の認証状態は解除されます（Web 認証では，この場合ログアウト画面は表示されません）。

(2) Web 認証と MAC 認証との共存時の認証優先

同一端末（同一 MAC アドレスを持つ端末）で，MAC 認証が先に認証成功した場合，Web 認証は認証エ

ラーとなります。また，Web 認証が先に認証成功した場合は，Web 認証の認証状態はそのままとなります（MAC 認証の認証はエラーとなります）。

5.3 レイヤ 2 認証共通の機能

レイヤ 2 認証共通の機能とその機能を設定するに当たり前提となる項目について説明します。

- 設定時の認証単位
- 認証前端末の通信許可
- 認証数制限
- 強制認証
- 認証済み端末のポート間移動
- RADIUS サーバ通信の dead interval 機能
- MAC ポートに dot1q 設定時の動作

5.3.1 設定時の認証単位

レイヤ 2 認証では，認証の設定を物理ポート単位または VLAN 単位に行います。どちらの単位で設定するかは，レイヤ 2 認証機能および認証モードによって異なります。

認証単位ごとのレイヤ 2 認証機能と認証モードを次の表に示します。

表 5-9 認証単位ごとのレイヤ 2 認証機能と認証モード

認証単位	レイヤ 2 認証機能と認証モード
物理ポート	• IEEE802.1X（ポート単位認証） • Web 認証（固定 VLAN モード） • Web 認証（ダイナミック VLAN モード） • MAC 認証（固定 VLAN モード） • MAC 認証（ダイナミック VLAN モード）
VLAN	• IEEE802.1X（VLAN 単位認証（静的）） • IEEE802.1X（VLAN 単位認証（動的）） • Web 認証（レガシーモード） • 認証 VLAN

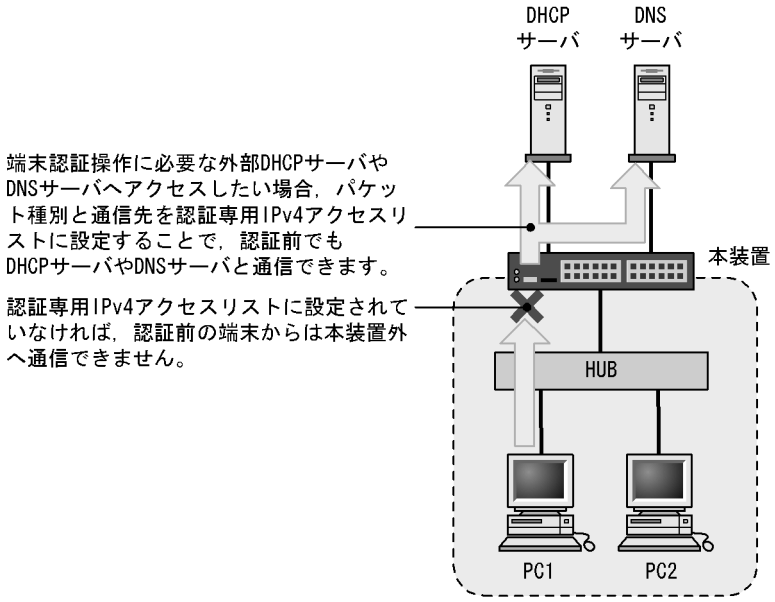
5.3.2 認証前端末の通信許可

(1) 認証専用 IPv4 アクセスリスト

認証前状態の端末に対して，DHCP サーバから IP アドレスの配布や DNS サーバによる名前解決ができるようにするには，認証前状態の端末が DHCP サーバや DNS サーバと通信できる必要があります。

認証前状態の端末が本装置外の装置（DHCP サーバや DNS サーバ）と通信できるようにするには，認証専用の IPv4 アクセスリスト（以降，**認証専用 IPv4 アクセスリスト**と呼びます）を認証前 VLAN に設定します。

図 5-5　認証専用 IPv4 アクセスリスト設定後の通信



認証専用 IPv4 アクセスリストは，通常のアクセスリスト（コンフィグレーションコマンド ip access-group など）とは異なり，認証後は設定されたフィルタ条件が適用されません。ただし，通常のアクセスリストで設定されたフィルタ条件は，認証専用 IPv4 アクセスリストで設定されたフィルタ条件よりも優先されます。認証対象ポートに通常のアクセスリストと認証専用 IPv4 アクセスリストを設定した場合，通常のアクセスリストのフィルタ条件が，認証前にも認証後にも適用されますので，認証専用 IPv4 アクセスリストに設定したフィルタ条件を通常のアクセスリストにも設定してください。

また，認証前の端末に本装置内蔵の DHCP サーバ機能から IP アドレスを配布する場合，および外部 DHCP サーバから IP アドレスを配布する場合，認証専用 IPv4 アクセスリストのフィルタ条件に，対象となる DHCP サーバ向けの DHCP パケットを通信させる設定が必要になります。この場合は，次に示すようにフィルタ条件を必ず設定してください。

［必要なフィルタ条件設定例］

DHCP サーバの IP アドレスが 10.10.10.254，認証対象端末のネットワークが 10.10.10.0/24 の場合

```
permit udp 10.10.10.0 0.0.0.255 host 10.10.10.254 eq bootps
permit udp host 0.0.0.0 host 10.10.10.254 eq bootps
permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
```

［認証専用 IPv4 アクセスリスト設定時の注意］

コンフィグレーションコマンド authentication ip access-group を設定する場合，次の点に注意してください。

- 指定できる認証専用 IPv4 アクセスリストは 1 個だけです。認証対象となるすべてのポートに，コンフィグレーションコマンド authentication ip access-group で同一の設定をしてください。
- 認証専用 IPv4 アクセスリストで設定できるフィルタ条件が収容条件を超えている場合，収容条件内のものだけ設定されます。
- コンフィグレーションコマンド permit または deny によって次のフィルタ条件が指定されても，適用されません。
  - tcp ポートの range 指定
  - udp ポートの range 指定
  - user-priority

- vlan

- 設定した条件以外のパケット廃棄設定は，本設定の収容条件数には含まれません。各認証プログラムで条件以外のパケット廃棄設定が暗黙に設定されます。
- 認証専用 IPv4 アクセスリストのフィルタ条件としてコンフィグレーションコマンド permit ip host <ip address> に認証端末の IP アドレスを設定した場合，コンフィグレーションコマンド authentication arp-relay を設定しなくても，認証前の端末から送信される ARP パケットは疎通します。
- Web 認証専用 IP アドレスは認証専用 IPv4 アクセスリストのフィルタ条件の宛先 IP アドレスの対象外となるため，宛先 IP アドレスとして Web 認証専用 IP アドレスが含まれる設定をした場合でも，Web 認証専用 IP アドレスでのログイン操作ができます。

(2) ARP パケットのリレー機能

認証前状態の端末から送信される ARP パケットは装置外へ転送できませんが，コンフィグレーションコマンド authentication arp-relay を設定すると，認証前状態の端末から送信された ARP パケットを装置外へ転送できます。

(3) 動作可能なレイヤ 2 認証

認証専用 IPv4 アクセスリストおよび ARP パケットのリレー機能が動作するレイヤ 2 認証を次の表に示します。

表 5-10 認証専用 IPv4 アクセスリストおよび ARP パケットのリレー機能が動作するレイヤ 2 認証

機能	IEEE802.1X			Web 認証			MAC 認証	
	ポート単位認証	VLAN 単位認証（静的）	VLAN 単位認証（動的）	固定 VLAN モード	ダイナミック VLAN モード	レガシーモード	固定 VLAN モード	ダイナミック VLAN モード
認証専用 IPv4 アクセスリスト	○	○	○	○	○	×	○	○
ARP パケットのリレー機能	○	○	○	○	○	×	○	○

（凡例） ○：動作できる　×：動作できない

(4) DHCP snooping 設定時の注意

認証対象のポートに DHCP snooping で untrust ポートが設定された場合，認証専用 IPv4 アクセスリストのフィルタ条件にプロトコル名称 bootps または bootpc を設定しても，端末から送信される DHCP パケットは DHCP snooping の対象となるため，DHCP snooping で許可された DHCP パケットだけが装置外へ送信されます。

また，端末から送信される ARP パケットは DHCP snooping の対象となるため，DHCP snooping で許可された ARP パケットは装置外へ送信されます。

(5) QoS との共存

認証専用 IPv4 アクセスリストおよび ARP パケットリレー機能と QoS（受信側）は，同一ポートで共存できません。

5.3.3 認証数制限

レイヤ 2 認証共通で認証数の制限を設定できます。

設定する単位を次に示します。

- ポート単位
- 装置単位

(1) ポート単位の認証数制限

コンフィグレーションコマンド authentication max-user で，ポート単位に認証数の制限を設定できます。各レイヤ 2 認証で認証された数がポート単位に設定された制限値を超えた場合，認証エラーとなります。

(2) 装置単位の認証数制限

コンフィグレーションコマンド authentication max-user で，装置単位に認証数の制限を設定できます。各レイヤ 2 認証で認証された合計数が装置単位に設定された制限値を超えた場合，認証エラーとなります。

(3) 認証数制限を設定できるレイヤ 2 認証

ポート単位の認証数制限，および装置単位の認証数制限を設定できるレイヤ 2 認証を次の表に示します。

表 5-11 認証数制限を設定できるレイヤ 2 認証

機能	IEEE802.1X			Web 認証			MAC 認証	
	ポート単位認証	VLAN 単位認証（静的）	VLAN 単位認証（動的）	固定 VLAN モード	ダイナミック VLAN モード	レガシーモード	固定 VLAN モード	ダイナミック VLAN モード
ポート単位の認証数制限	○※1	○※1	○※2	○	○	×	○	○
装置単位の認証数制限	○※1	○※1	○※2	○	○	×	○	○

（凡例） ○：設定できる　×：設定できない

注※ 1

疎通制限されている認証端末は対象外です。詳細については，「6.2.9　認証端末の疎通制限」を参照してください。

注※ 2

コンフィグレーションによって，対象になる場合とならない場合があります。詳細については，「6.2.8　VLAN 単位認証（動的）の動作モード」を参照してください。

5.3.4 強制認証

コンフィグレーションコマンド authentication force-authorized enable が設定された場合，次に示すどちらかの状態が発生すると，すべてのログイン要求を認証成功とします。

● RADIUS 認証方式で，設定された RADIUS サーバからの応答がなくなったとき

● ローカル認証方式で，装置内蔵の認証データが 1 件も登録されていないとき
- Web 認証の場合は，内蔵 Web 認証 DB に 1 件もユーザ登録がないとき

- MAC 認証の場合は，内蔵 MAC 認証 DB に 1 件も MAC アドレス登録がないとき

強制認証されたユーザに対しては，認証が解除されるまで通常の認証成功と同様に扱います。強制認証が動作する認証モードを次の表に示します。

表 5-12　強制認証が動作する認証モード

機能	IEEE802.1X			Web 認証			MAC 認証	
	ポート単位認証	VLAN 単位認証（静的）	VLAN 単位認証（動的）	固定 VLAN モード	ダイナミック VLAN モード	レガシーモード	固定 VLAN モード	ダイナミック VLAN モード
強制認証	×	×	×	○	○※	×	○	○※

（凡例）　○：動作できる　×：動作できない

注※

ダイナミック VLAN モードの場合，強制認証で切り替える VLAN ID をコンフィグレーションコマンド authentication force-authorized vlan で指定します。なお，コンフィグレーションコマンド authentication force-authorized vlan が省略された場合は，ネイティブ VLAN の VLAN ID に切り替えます。

［強制認証設定時の注意］

強制認証は，セキュリティ上の問題となるおそれがありますので，使用する際は十分に検討してください。

例：MAC 認証専用 RADIUS サーバ使用時

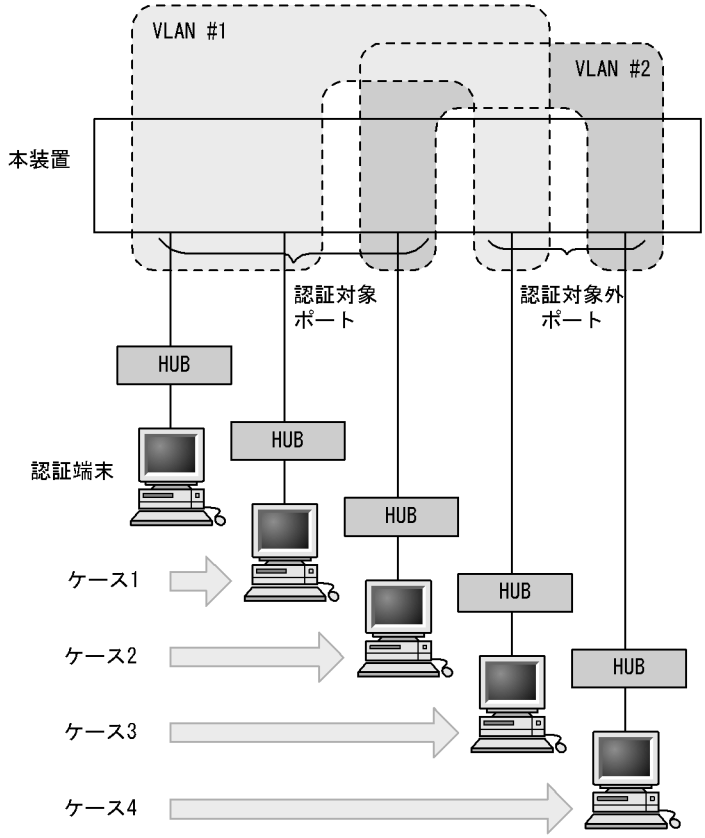
強制認証，および同一ポートに Web 認証と MAC 認証を同時に設定し，さらに，MAC 認証専用 RADIUS サーバが設定されている場合，MAC 認証専用 RADIUS サーバへ通信できないために強制認証が動作すると，MAC 認証の強制認証動作によって，Web 認証の認証対象端末も Web 認証をしなくても通信できるため注意してください。

5.3.5　認証済み端末のポート間移動

レイヤ 2 認証で認証された端末をほかのポートに移動した場合，ポートの状態や認証状態がどのように変わるか説明します。

認証済み端末のポート間移動には次の図に示す四つのケースがあります。

図 5-6　認証済み端末のポート間移動例



なお，MAC VLAN を使用した場合，次のようにケース 1 とケース 2 を判定します。

ケース 1：

移動先の認証対象ポートで，次のどちらかの条件を満たしている場合に同一の VLAN への移動と見なします。

- コンフィグレーションコマンド switchport mac vlan で同じ VLAN ID が設定されている
- レイヤ 2 認証によって動的に同じ VLAN ID がすでに登録されている

また，動的に MAC VLAN の VLAN ID が登録されていない場合は，Web 認証または MAC 認証で認証済みの端末が移動するときに端末が所属している VLAN ID が作成されるため，同一の VLAN への移動と見なします。

ケース 2：

移動先の認証対象ポートで，次の条件を満たしている場合に異なる VLAN への移動と見なします。

- コンフィグレーションコマンド switchport mac vlan で異なる VLAN ID が設定されている

また，動的に MAC VLAN の VLAN ID が登録されていない場合に IEEE802.1X の端末が移動するときは，異なる VLAN への移動と見なします。

これら四つのケースについて，レイヤ 2 認証ごとに説明します。

(1) IEEE802.1X でのポート間移動時の動作

IEEE802.1X で認証された端末がポートを移動した場合のポートや認証の状態について，認証モードごとに次の表に示します。

表 5-13 IEEE802.1X でのポート間移動時の動作（ポート単位認証）

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	移動後，再認証操作	ポート情報が更新	移動前の認証解除	移動後に認証されるまで通信不可
2	認証対象ポート	別 VLAN	移動後，再認証操作	未更新	認証状態が残る	移動後に認証されるまで通信不可
3	認証対象外ポート	同一 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

表 5-14 IEEE802.1X でのポート間移動時の動作（VLAN 単位認証（静的））

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続する	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	移動後，再認証操作	未更新	認証状態が残る	移動後に認証されるまで通信不可
3	認証対象外ポート	同一 VLAN	－	－	－	－
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

（凡例）

－：VLAN 単位認証（静的）は VLAN 単位での設定のため，同一 VLAN に認証対象外ポートはありません

表 5-15 IEEE802.1X でのポート間移動時の動作（VLAN 単位認証（動的））

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続する	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	移動後，再認証操作	削除	移動前の認証解除	移動後に認証されるまで通信不可
3	認証対象外ポート	同一 VLAN	－	－	－	－
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

（凡例）

－：VLAN 単位認証（動的）は VLAN 単位での設定のため，同一 VLAN に認証対象外ポートはありません

（2） Web 認証でのポート間移動時の動作

Web 認証で認証された端末がポートを移動した場合のポートや認証の状態について，認証モードごとに次

の表に示します。

表 5-16 Web 認証でのポート間移動時の動作（固定 VLAN モード）

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続される	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	移動後に認証されるまで通信不可
3	認証対象外ポート	同一 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

表 5-17 Web 認証でのポート間移動時の動作（ダイナミック VLAN モード）

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続される	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
3	認証対象外ポート	同一 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

表 5-18 Web 認証でのポート間移動時の動作（レガシーモード）

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続される	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
3	認証対象外ポート	同一 VLAN	－	－	－	－
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

（凡例）

－：Web 認証（レガシーモード）は VLAN 単位での設定のため，同一 VLAN に認証対象外ポートはありません

（3） MAC 認証でのポート間移動時の動作

MAC 認証で認証された端末がポートを移動した場合のポートや認証の状態について，認証モードごとに次の表に示します。

表 5-19 MAC 認証でのポート間移動時の動作（固定 VLAN モード）

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続される	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	移動後，再認証※	削除※	移動前の認証解除※	移動後に認証されるまで通信不可※
3	認証対象外ポート	同一 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

注※
認証済み端末からポート移動後にブロードキャスト ARP パケットが送信された場合の動作です。ブロードキャスト ARP パケット以外のパケットでは，認証解除されないで認証状態が残ります。

表 5-20 MAC 認証でのポート間移動時の動作（ダイナミック VLAN モード）

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続される	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	認証解除※	削除※	移動前の認証解除※	移動後に認証されるまで通信不可※
3	認証対象外ポート	同一 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

注※
認証済み端末からポート移動後にブロードキャスト ARP パケットが送信された場合の動作です。ブロードキャスト ARP パケット以外のパケットでは，認証解除されないで認証状態が残ります。

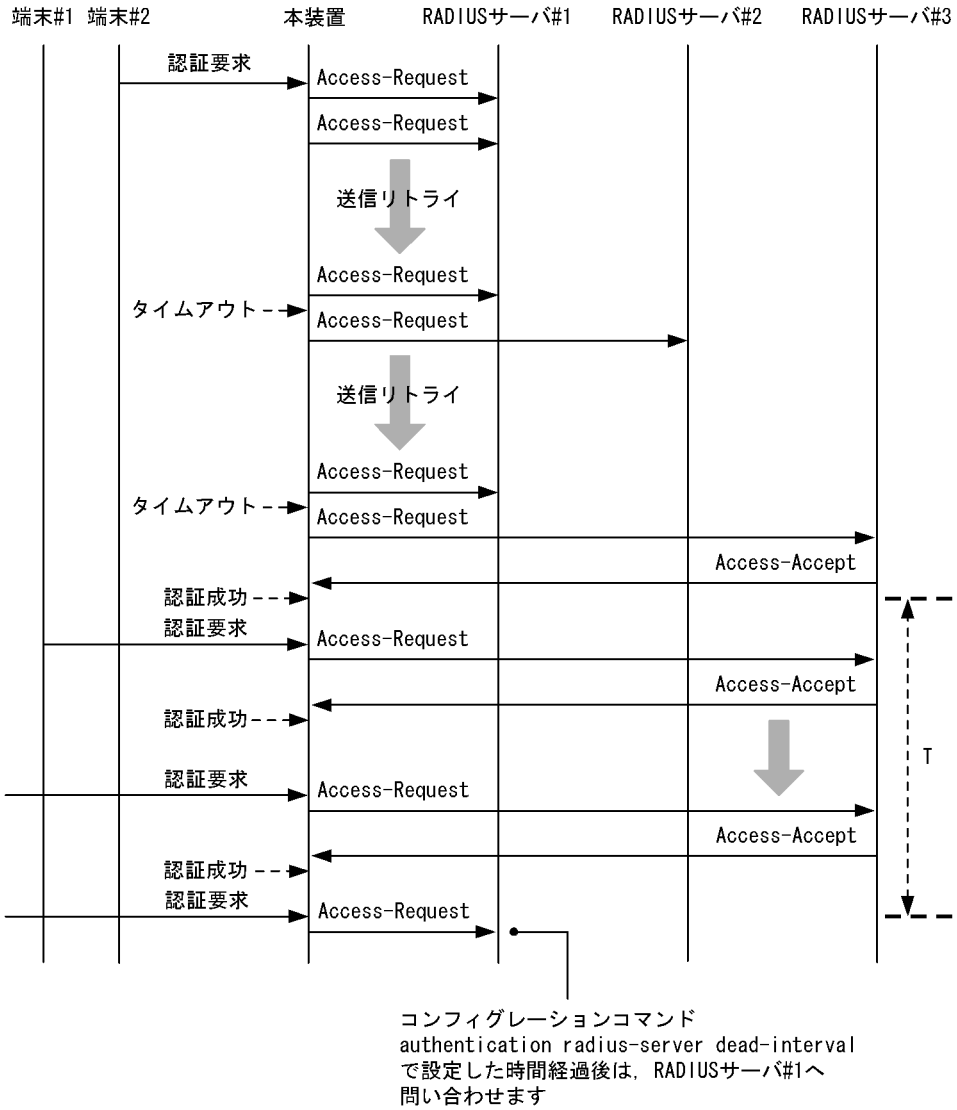
5.3.6 RADIUS サーバ通信の dead interval 機能

RADIUS サーバが無応答になったあと，コンフィグレーションコマンド authentication radius-server dead-interval で設定された時間の間，ほかの RADIUS サーバと通信して認証を実施します。また，設定された時間が経過したあとは，最初に設定した RADIUS サーバを使用して認証を実施します。また，設定されたすべての RADIUS サーバが無応答となった場合，コンフィグレーションコマンド authentication radius-server dead-interval で設定された時間の間は，RADIUS サーバとの通信が復旧しても認証失敗となります。なお，dead-interval 機能で認証失敗となった状態から最初に設定した RADIUS サーバへ通信状態に戻す場合は，次の運用コマンドを実行してください。

- Web 認証：clear web-authentication dead-interval-timer
- MAC 認証：clear mac-authentication dead-interval-timer

RADIUS サーバ通信の dead interval 機能を次の図に示します。

図 5-7 RADIUS サーバ通信の dead interval 機能



T：コンフィグレーションコマンドauthentication radius-server dead-intervalでの設定時間

RADIUS サーバ通信の dead-interval 機能とレイヤ 2 認証の対応を次の表に示します。

表 5-21 RADIUS サーバ通信の dead-interval 機能とレイヤ 2 認証の対応

機能	IEEE802.1X			Web 認証			MAC 認証	
	ポート単位認証	VLAN 単位認証（静的）	VLAN 単位認証（動的）	固定 VLAN モード	ダイナミック VLAN モード	レガシーモード	固定 VLAN モード	ダイナミック VLAN モード
RADIUS サーバ通信の dead interval 機能	×	×	×	○	○	×	○	○

（凡例） ○：対応する ×：対応しない

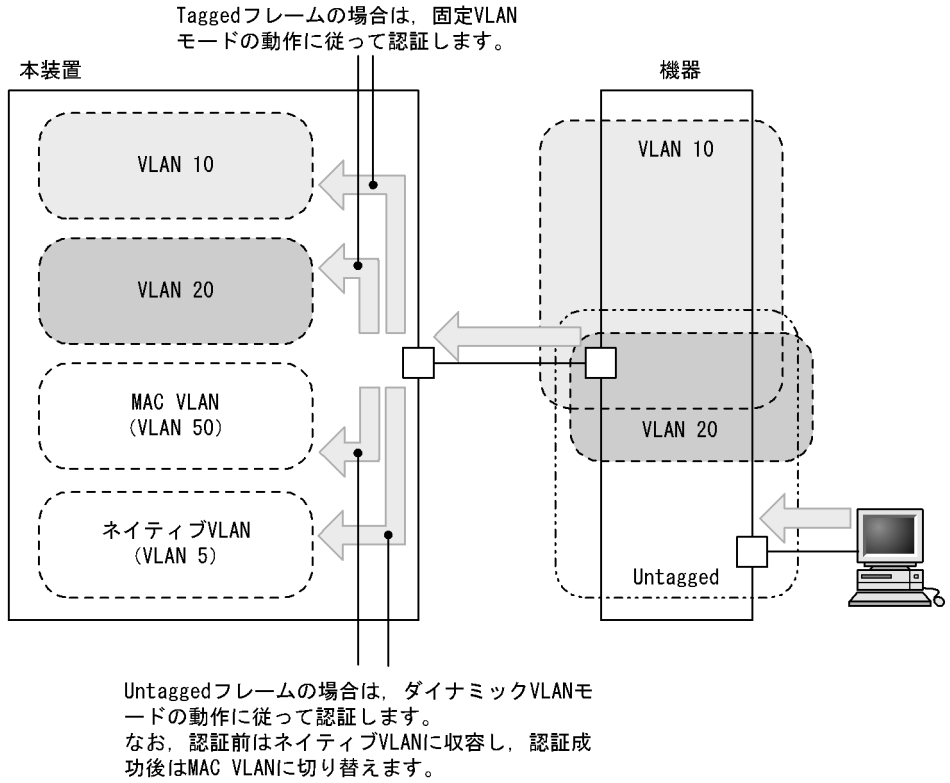
5.3.7 MAC ポートに dot1q 設定時の動作

MAC ポートにコンフィグレーションコマンド switchport mac dot1q vlan で dot1q が設定されている場合，Tagged フレームは固定 VLAN モードの動作に従って認証されます。

Untagged フレームはダイナミック VLAN モードの動作に従って認証されます。なお，Untagged フレームは認証前はネイティブ VLAN に収容され，認証成功後に認証後の VLAN ID に切り替わります。

MAC ポートに dot1q が設定されている場合の動作を次の図に示します。

図 5-8 MAC ポートに dot1q が設定されている場合の動作



また，該当ポートにコンフィグレーションコマンド mac-authentication dot1q-vlan force-authorized が設定されている場合，Tagged フレームに対しては認証除外と判断し，MAC 認証をしないで通信できます。

ただし，認証除外機能で適用された端末は MAC 認証の認証端末として扱われるため，次のことに注意してください。

- 認証除外端末（MAC アドレス）は，該当ポートに設定された認証制限数に含まれます。
- 認証除外端末が解除された時，ログアウトを意味する動作ログメッセージが表示されます。また，認証除外端末をポート間で移動する場合も，いったん認証除外端末が解除されるため，ログアウトを意味する動作ログメッセージが表示されます。
- 次の契機で認証除外を解除します。
  - 運用コマンドによる認証除外解除
    運用コマンド clear mac-authentication auth-state で認証除外端末の MAC アドレスを指定すると認証除外を解除します。
    また，運用コマンド clear mac-authentication auth-state ですべての MAC 認証済み端末を解除する

オプションを指定した場合も，認証除外を解除します。

- 認証除外端末接続ポートのリンクダウンによる認証除外解除
  認証除外端末が接続しているポートのリンクダウンを検出した際に，該当するポートに接続された端末の認証除外を解除します。
- 認証除外端末の MAC アドレステーブルエージングによる認証除外解除
  認証除外端末の MAC アドレステーブルのエージング時間経過後約 10 分間，認証除外端末からのアクセスがない状態が続いた場合に，認証除外を解除します。
- VLAN 設定変更による認証除外解除
  コンフィグレーションコマンドで認証除外端末が含まれる VLAN の設定を変更した場合，認証除外を解除します。
  ［コンフィグレーションの変更内容］
  ・VLAN を削除した場合
  ・VLAN を停止（suspend）した場合
- 認証モード切替による認証除外解除
  copy コマンドでコンフィグレーションを変更して，認証モードが切り替わる設定をした場合，認証除外を解除します。
- MAC 認証の停止による認証除外解除
  コンフィグレーションコマンド no mac-authentication system-auth-control で MAC 認証の設定が削除されて MAC 認証が停止した場合，認証除外を解除します。

MAC ポートに dot1q が設定されている場合のレイヤ 2 認証の動作を次の表に示します。

表 5-22　MAC ポートに dot1q が設定されている場合のレイヤ 2 認証の動作

受信フレーム	IEEE802.1X	Web 認証	MAC 認証
Untagged フレーム	VLAN 単位認証（動的）で認証	ダイナミック VLAN モードで認証	ダイナミック VLAN モードで認証
Tagged フレーム	VLAN 単位認証（静的）で認証	認証できない	固定 VLAN モードで認証

5.4 レイヤ 2 認証使用時の注意事項

5.4.1 本装置の設定および状態変更時の注意

(1) set clock コマンドを使用する際の注意

認証接続時間を装置の時刻を用いて管理しているので，運用コマンド set clock で日時を変更した場合，認証接続時間に影響が出ます。

例えば，3 時間後の時刻に値を変更した場合，認証接続時間が 3 時間経過した状態となります。また，逆に 3 時間前の時刻に値を変更した場合は，認証接続時間が 3 時間延長されます。

5.4.2 RADIUS サーバ使用時の注意

(1) RADIUS サーバの設定でホスト名を指定した場合の注意事項

RADIUS サーバをホスト名で指定した場合，DNS サーバへ接続できないなどの理由によって名前解決ができない環境では，次に示す現象が発生することがあります。

● 運用コマンドを実行した場合
- 実行結果の表示が遅くなります。
- 表示が途中で止まり，しばらくして継続表示されます。
- IEEE802.1X では，「Connection failed to 802.1X program.」が表示されます。
- Web 認証および MAC 認証では，「Can't execute.」が表示されます。

● コンフィグレーションコマンドを実行した場合
- コンフィグレーションの保存またはコンフィグレーションの反映に時間が掛かる場合があります。

● SNMP マネージャによる IEEE802.1X MIB 情報を取得する場合
- 応答が遅くなる，または SNMP 受信タイムアウトになります。

上記の現象を避けるため，RADIUS サーバの設定に IPv4 アドレスまたは IPv6 アドレスで指定することを推奨します。ホスト名での指定が必要な場合は，必ず DNS サーバからの応答があることを確認してください。

(2) IEEE802.1X で RADIUS サーバとの通信が切れた場合の注意事項

IEEE802.1X では，RADIUS サーバとの通信が切れた場合，またはコンフィグレーションコマンド radius-server host で設定された RADIUS サーバが存在しない場合，ログイン要求 1 件づつに対して，コンフィグレーションコマンド radius-server timeout で指定されたタイムアウト時間およびコンフィグレーションコマンド radius-server retransmit で設定された再送回数分だけの時間が掛かるため，1 ログイン要求当たりの認証処理に時間が掛かります。

また，複数の RADIUS サーバが設定された場合でも，コンフィグレーションコマンド radius-server host の順にログインごとに毎回アクセスするため，先に設定された RADIUS サーバで障害などによって通信ができなくなると，認証処理に時間が掛かります。

このようなときは，ログイン操作をいったん止め，コンフィグレーションコマンド radius-server host で正常な RADIUS サーバを設定し直したあとに，ログイン操作を行ってください。

5.5 レイヤ 2 認証共通コンフィグレーション

5.5.1 コンフィグレーションコマンド一覧

レイヤ 2 認証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 5-23 コンフィグレーションコマンド一覧

コマンド名	説明	適用するレイヤ 2 認証		
		IEEE802.1X	Web 認証※	MAC 認証
authentication arp-relay	認証前状態の端末からの ARP パケットを本装置の外部に転送したい場合に指定します。	○	○	○
authentication force-authorized enable	強制認証を設定します。	－	○	○
authentication force-authorized vlan	ダイナミック VLAN モードの強制認証時に切り替える VLAN ID を指定します。	－	○	○
authentication ip access-group	認証前状態の端末からのパケットを本装置の外部に転送したい場合，転送したいパケット種別を IPv4 アクセスリストで指定します。	○	○	○
authentication max-user (global)	装置単位の認証数制限値を設定します。	○	○	○
authentication max-user (interface)	ポート単位の認証数制限値を設定します。	○	○	○
authentication radius-server dead-interval	RADIUS サーバ無応答時に再度，最優先 RADIUS サーバへアクセスするまでの待ち時間を設定します。	－	○	○

（凡例） ○：設定可 －：設定不可
注※ Web 認証は固定 VLAN モードおよびダイナミック VLAN モードで適用します。

5.5.2 レイヤ 2 認証共通コンフィグレーションコマンドのパラメータ設定

(1) 認証前状態端末からの ARP パケットを本装置外部に転送する設定

[設定のポイント]

認証前状態の端末から送信された ARP パケットを本装置外部に転送する設定をします。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/10**
   (config-if)# web-authentication port
   (config-if)# mac-authentication port

```
(config-if)# authentication arp-relay
(config-if)# exit
```

Web 認証と MAC 認証の認証対象ポート 0/10 に ARP パケットを転送するよう設定します。

(2) 認証専用 IPv4 アクセスリストの設定

[設定のポイント]

認証前状態の端末から本装置の外部への通信を許可する認証専用 IPv4 アクセスリストを設定します。

[コマンドによる設定]

1.
```
(config)# ip access-list extended 100
(config-ext-nacl)# permit udp any any eq bootps
(config-ext-nacl)# permit ip any host 10.0.0.1
(config-ext-nacl)# exit
(config)# interface gigabitethernet 0/10
(config-if)# web-authentication port
(config-if)# mac-authentication port
(config-if)# authentication ip access-group 100
(config-if)# exit
```

認証前の端末から DHCP パケットと IP アドレス 10.0.0.1（DNS サーバ）へのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。

(3) 強制認証の設定

[設定のポイント]

RADIUS サーバが応答しない場合，または Web 認証では内蔵 Web 認証 DB が，MAC 認証では内蔵 MAC 認証 DB が登録されていない場合に強制認証する設定をします。

[コマンドによる設定]

1.
```
(config)# authentication force-authorized enable
```

強制認証を設定します。

(4) 強制認証時に切り替える VLAN ID の設定

[設定のポイント]

ダイナミック VLAN モードで強制認証となった場合に切り替える VLAN ID を設定します。

[コマンドによる設定]

1.
```
(config)# interface gigabitethernet 0/5
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 100,200
(config-if)# web-authentication port
(config-if)# mac-authentication port
(config-if)# authentication force-authorized vlan 100
(config-if)# exit
```

Web 認証と MAC 認証のダイナミック VLAN モードで指定された認証対象ポート 0/5 に，強制認証時

に切り替える VLAN ID 100 を設定します。

(5) 装置単位の認証数制限値の設定

[設定のポイント]

レイヤ 2 認証の装置単位の認証数制限を設定します。

[コマンドによる設定]

1. **(config)# authentication max-user 512**
   レイヤ 2 認証の装置単位の認証数制限を 512 に設定します。

(6) ポート単位の認証数制限値の設定

[設定のポイント]

レイヤ 2 認証のポート単位の認証数制限を設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/5**
   (config-if)# switchport mode access
   (config-if)# switchport vlan 10
   (config-if)# web-authentication port
   (config-if)# mac-authentication port
   (config-if)# authentication max-user 64
   (config-if)# exit
   認証対象ポート 0/5 の認証数制限を 64 に設定します。

(7) RADIUS サーバへアクセス時の dead interval 時間の設定

[設定のポイント]

最優先 RADIUS サーバが無応答になったあと，ほかの RADIUS サーバで認証を始めてから，再度最優先 RADIUS サーバへアクセスを試みるまでの待ち時間 (dead interval 時間) を設定します。

[コマンドによる設定]

1. **(config)# authentication radius-server dead-interval 20**
   RADIUS サーバの dead interval 時間を 20 分に設定します。

6 IEEE802.1X の解説

IEEE802.1X は OSI 階層モデルの第 2 レイヤで認証を行う機能です。この章では IEEE802.1X の概要について説明します。

6.1 IEEE802.1X の概要

IEEE802.1X は，不正な LAN 接続を規制する機能です。バックエンドに認証サーバ（一般的には RADIUS サーバ）を設置し，認証サーバによる端末の認証が通過した上で，本装置の提供するサービスを利用できるようにします。

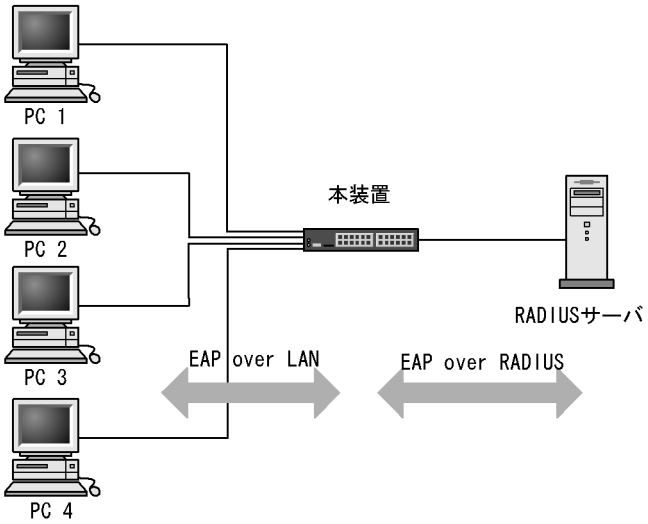
IEEE802.1X の構成要素と動作概略を次の表に示します。

表 6-1 構成要素と動作概略

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

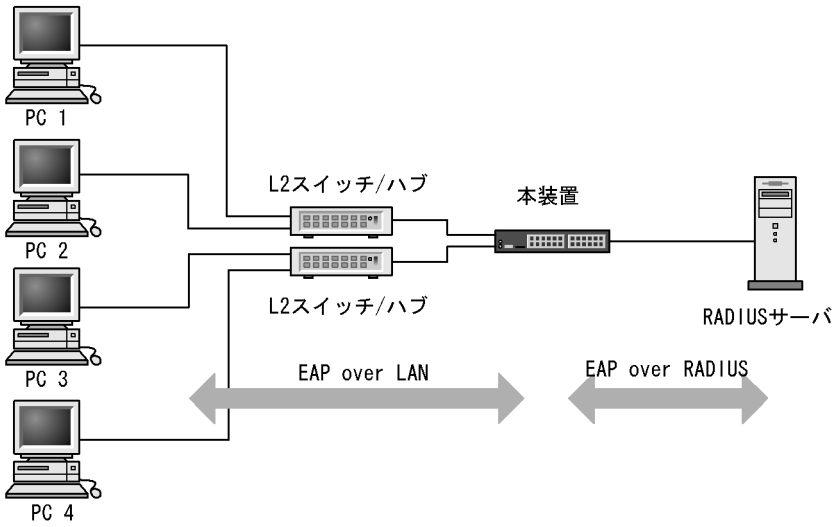
標準的な IEEE802.1X の構成では，本装置のポートに直接端末を接続して運用します。本装置を使った IEEE802.1X 基本構成を次の図に示します。

図 6-1 IEEE802.1X 基本構成



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

図 6-2 端末との間に L2 スイッチを配置した IEEE802.1X 構成



6.1.1 サポート機能

本装置でサポートする機能を以下に示します。

(1) 認証動作モード

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

(2) 認証方式

本装置でサポートする認証方式は RADIUS サーバ認証です。端末から受信した EAPOL パケットを EAPoverRADIUS に変換し，認証処理は RADIUS サーバで行います。RADIUS サーバは EAP 対応されている必要があります。

本装置が使用する RADIUS の属性名を「表 6-2 認証で使用する属性名（その 1 Access-Request)」から「表 6-5 認証で使用する属性名（その 4 Access-Reject)」に示します。

表 6-2 認証で使用する属性名（その 1 Access-Request）

属性名	Type 値	説明
User-Name	1	認証されるユーザ名。
NAS-IP-Address	4	認証を要求している，Authenticator(本装置) の IP アドレス。ローカルアドレスが設定されている場合はローカルアドレス，ローカルアドレスが設定されていない場合は，送信インタフェースの IP アドレス。
NAS-Port	5	Supplicant を認証している認証単位の IfIndex。
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。
Framed-MTU	12	Supplicant ～ Authenticator 間の最大フレームサイズ。 (1466) 固定。
State	24	Authenticator と RADIUS サーバ間の State 情報の保持を可能にする。
Called-Station-Id	30	ブリッジやアクセスポイントの MAC アドレス。本装置の MAC アドレス (ASCII，"-" 区切り)。

属性名	Type 値	説明
Calling-Station-Id	31	Supplicant の MAC アドレス（ASCII，"-" 区切り）。
NAS-Identifier	32	Authenticator を識別する文字列（ホスト名の文字列）。
NAS-Port-Type	61	Authenticator がユーザ認証に使用している，物理ポートのタイプ。 Ethernet(15) 固定。
Connect-Info	77	Supplicant のコネクションの特徴を示す文字列。 ポート単位認証： 物理ポート（“ CONNECT Ethernet ”） CH ポート（“ CONNECT Port-Channel ”） VLAN 単位認証（静的）：（“ CONNECT VLAN ”） VLAN 単位認証（動的）：（“ CONNECT DVLAN ”）
EAP-Message	79	EAP パケットをカプセル化する。
Message-Authenticator	80	RADIUS/EAP パケットを保護するために使用する。
NAS-Port-Id	87	Supplicant を認証する Authenticator のポートを識別するための文字列。 ポート単位認証：“ Port x/y ”，“ ChGr x ” VLAN 単位認証（静的）：“ VLAN x ” VLAN 単位認証（動的）：“ DVLAN x ” （x，y には数字が入る）
NAS-IPv6-Address	95	認証を要求している，Authenticator（本装置）の IPv6 アドレス。ローカルアドレスが設定されている場合はローカルアドレス，ローカルアドレスが設定されていない場合は送信インタフェースの IPv6 アドレス。ただし，IPv6 リンクローカルアドレスで通信する場合は，ローカルアドレス設定の有無にかかわらず送信インタフェースの IPv6 リンクローカルアドレス。

表 6-3　認証で使用する属性名（その 2　Access-Challenge）

属性名	Type 値	説明
Reply-Message	18	ユーザに表示されるメッセージ。
State	24	Authenticator と RADIUS サーバ間の State 情報の保持を可能にする。
Session-Timeout	27	Supplicant へ送信した EAP-Request に対する応答待ちタイムアウト値。
EAP-Message	79	EAP パケットをカプセル化する。
Message-Authenticator	80	RADIUS/EAP パケットを保護するために使用する。

表 6-4　認証で使用する属性名（その 3　Access-Accept）

属性名	Type 値	説明
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。
Filter-Id	11	Supplicant のセッションに適用されるフィルタ・リストの名前。 ポート単位認証の端末認証モード，および VLAN 単位認証（静的）でだけ意味を持つ。ただし，適用可能なフィルタが認証専用 IPv4 アクセスリスト固定であるため，"0" 以外の値が設定されていた場合に有効。
Reply-Message	18	ユーザに表示されるメッセージ。
Session-Timeout	27	Supplicant の再認証タイマ値。※
Termination-Action	29	Radius サーバからの再認証タイマ満了時のアクション指示。※
Tunnel-Type	64	トンネル・タイプ。VLAN 単位認証（動的）でだけ意味を持つ。 VLAN(13) 固定。

属性名	Type 値	説明
Tunnel-Medium-Type	65	トンネルを作成する際のプロトコル。VLAN 単位認証 (動的) でだけ意味を持つ。 IEEE802(6) 固定。
EAP-Message	79	EAP パケットをカプセル化する。
Message-Authenticator	80	RADIUS/EAP パケットを保護するために使用する。
Tunnel-Private-Group-ID	81	VLAN を識別する文字列。Accept 時は，認証済みの Supplicant に割り当てる VLAN を意味する。 VLAN 単位認証 (動的) でだけ意味を持つ。 次に示す文字列が対応する。 (1)VLAN ID を示す文字列 (2)"VLAN"+VLAN ID を示す文字列 (3) コンフィグレーションコマンド name で指定した VLAN 名称を示す文字列 文字列にスペースを含んではいけない（含めた場合 VLAN 割り当ては失敗する）。 （設定例） VLAN10 の場合 (1) の場合　"10" (2) の場合　"VLAN10" (3) の場合　"business-office"
Acct-Interim-Interval	85	Interim パケット送信間隔 (秒)。 60 以上を設定すると Interim パケットが送信される (60 未満では送信しない)。 この値を設定する場合，600 以上にすることを推奨する。600 未満にした場合ネットワークのトラフィックが増大するため注意が必要である。

注※

RADIUS から返送される Access-Accept で Termination-Action が Radius-Request(1) の場合，同時に設定された Session-Timeout の値が，再認証するまでの時間（単位：秒）となります。なお，Session-Timeout の値によって次に示す動作となります。

0　　：再認証は無効となります。

1 ～ 60　：再認証タイマ値を 60 秒として動作します。

61 ～ 65535：設定された値で動作します。

表 6-5　認証で使用する属性名（その 4　Access-Reject）

属性名	Type 値	説明
Reply-Message	18	ユーザに表示されるメッセージ。
EAP-Message	79	EAP パケットをカプセル化する。
Message-Authenticator	80	RADIUS/EAP パケットを保護するために使用する。

(3) 認証アルゴリズム

本装置でサポートする認証アルゴリズムを次の表に示します。

表 6-6　サポートする認証アルゴリズム

認証アルゴリズム	概要
EAP-MD5-Challenge	UserPassword とチャレンジ値の比較を行う。
EAP-TLS	証明書発行機構を使用した認証方式。
EAP-PEAP	EAP-TLS トンネル上で，ほかの EAP 認証アルゴリズムを用いて認証する。

認証アルゴリズム	概要
EAP-TTLS	EAP-TLS トンネル上で，他方式 (EAP，PAP，CHAP など) の認証アルゴリズムを用いて認証する。

(4) RADIUS Accounting 機能

本装置は RADIUS Accounting 機能をサポートします。この機能は IEEE802.1X 認証で認証許可となった端末へのサービス開始やサービス停止のタイミングでユーザアカウンティング情報を送信し，利用状況追跡を行えるようにするための機能です。RADIUS Authentication サーバと RADIUS Accounting サーバを別のサーバに設定することによって，認証処理とアカウンティング処理の負荷を分散させることができます。

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

表 6-7 RADIUS Accounting がサポートする属性

属性名	Type 値	解説	アカウンティング要求種別による送信の有無		
			start	stop	Interim-Update
User-Name	1	認証されるユーザ名。	○	○	○
NAS-IP-Address	4	認証を要求している，Authenticator(本装置) の IP アドレス。 ローカルアドレスが設定されている場合はローカルアドレス，ローカルアドレスが設定されていない場合は，送信インタフェースの IP アドレス。	○	○	○
NAS-Port	5	Supplicant を認証している認証単位の IfIndex。	○	○	○
Service-Type	6	提供するサービスタイプ。 Framed(2) 固定。	○	○	○
Calling-Station-Id	31	Supplicant の MAC アドレス（ASCII，"-" 区切り)。	○	○	○
NAS-Identifier	32	Authenticator を識別する文字列。(ホスト名の文字列)	○	○	○
Acct-Status-Type	40	Accounting 要求種別 Start(1)，Stop(2)，Interim-Update(3)	○	○	○
Acct-Delay-Time	41	Accounting 情報送信遅延時間 (秒)	○	○	○
Acct-Input-Octets	42	Accounting 情報 (受信オクテット数)。 (0) 固定。	−	○	○
Acct-Output-Octets	43	Accounting 情報 (送信オクテット数)。 (0) 固定。	−	○	○
Acct-Session-Id	44	Accounting 情報を識別する ID。	○	○	○
Acct-Authentic	45	認証方式 (RADIUS(1)，Local(2)，Remote(3))	○	○	○
Acct-Session-Time	46	Accounting 情報 (セッション持続時間)	−	○	○
Acct-Input-Packets	47	Accounting 情報 (受信パケット数)。 (0) 固定。	−	○	○
Acct-Output-Packets	48	Accounting 情報 (送信パケット数)。 (0) 固定。	−	○	○

属性名	Type 値	解説	アカウンティング要求種別による送信の有無		
			start	stop	Interim-Update
Acct-Terminate-Cause	49	Accounting 情報 (セッション終了要因) 詳細は,「表 6-8　Acct-Terminate-Cause での切断要因」を参照。 User Request (1), Lost Carrier (2), Admin Reset (6), Reauthentication Failure (20), Port Reinitialized (21)	―	○	―
NAS-Port-Type	61	Authenticator がユーザ認証に使用している,物理ポートのタイプ。 Ethernet(15) 固定。	○	○	○
NAS-Port-Id	87	Supplicant を認証する Authenticator のポートを識別するために使用する。 NAS-Port-Id は,可変長のストリングであり,NAS-Port が長さ 4 オクテットの整数値である点で NAS-Port と異なる。 ポート単位認証 :“ Port x/y ”,“ ChGr x ” VLAN 単位認証 (静的) :“ VLAN x ” VLAN 単位認証 (動的) :“ DVLAN x ” (x, y には数字が入る)	○	○	○
NAS-IPv6-Address	95	認証を要求している,Authenticator(本装置) の IPv6 アドレス。ローカルアドレスが設定されている場合はローカルアドレス,ローカルアドレスが設定されていない場合は,送信インタフェースの IPv6 アドレス。ただし,IPv6 リンクローカルアドレスで通信する場合は,ローカルアドレス設定の有無にかかわらず送信インタフェースの IPv6 リンクローカルアドレス。	○	○	○

(凡例) ○ : 送信する　― : 送信しない

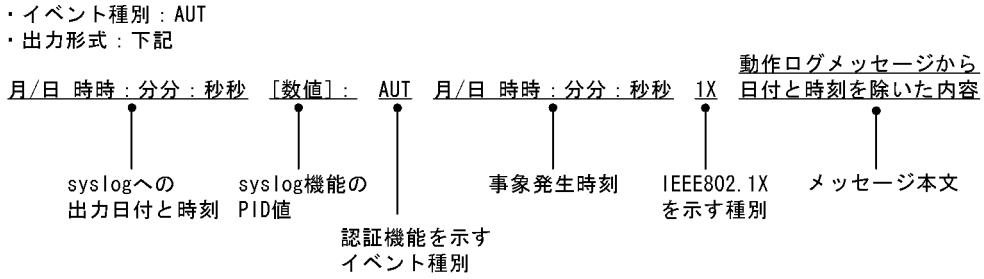
表 6-8　Acct-Terminate-Cause での切断要因

切断要因	値	解説
User Request	1	Supplicant からの要求で切断した。 • 認証端末から logoff を受信した場合
Lost Carrier	2	モデムのキャリア信号がなくなった。 • 内部エラー
Admin Reset	6	管理者の意思で切断した。 • 認証単位でコンフィグレーションを削除した場合 • force-authorized を設定した場合 • force-unauthorized を設定した場合 • force-authorized-port を設定した場合
Reauthentication Failure	20	再認証に失敗した。
Port Reinitialized	21	ポートの MAC が再初期化された。 • リンクダウンした場合 • clear dot1x auth-state を実行した場合

(5) syslog サーバへの動作ログ記録

IEEE802.1X の内部動作ログを syslog サーバに出力できます。なお，内部動作ログと同じ項目が出力されます。syslog サーバへの出力形式を次の図に示します。

図 6-3 syslog サーバへの出力形式



また，コンフィグレーションコマンド dot1x logging enable および logging event-kind によって，出力を開始および停止できます。

6.2 拡張機能の概要

本装置では，標準的な IEEE802.1X に対して機能拡張を行っています。拡張機能の概要を以下に示します。

6.2.1 認証モード

本装置の IEEE802.1X では，三つの基本認証モードとその下に三種類の認証サブモードを設けています。基本認証モードは，認証制御を行う単位を示し，認証サブモードは認証のさせ方を指定します。また，基本認証モードと認証サブモードに対して設定可能なオプションを設けています。各認証モードの関係を次の表に示します。

表 6-9 認証モードとオプションの関係

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

(凡例) －：該当なし

本装置の IEEE802.1X では，チャネルグループについても一つの束ねられたポートとして扱います。この機能での「ポート」の表現には通常のポートとチャネルグループを含むものとします。

(1) 基本認証モード

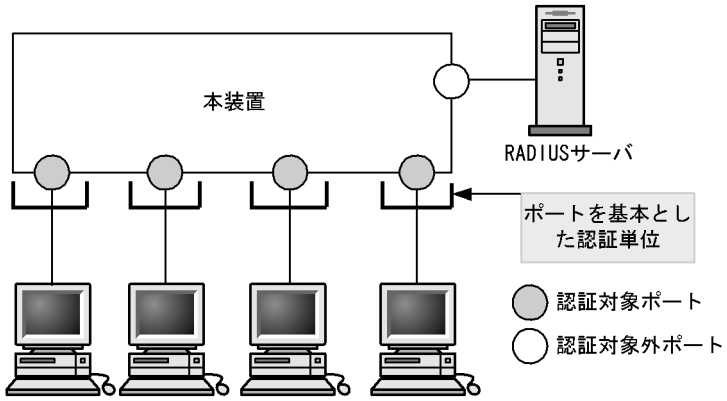
本装置でサポートする基本認証モードを以下に示します。

(a) ポート単位認証

認証の制御を物理ポートまたはチャネルグループに対して行います。IEEE802.1X の標準的な認証単位です。この認証モードでは IEEE 802.1Q VLAN-Tag の付与された EAPOL フレームを扱うことはできません。IEEE 802.1Q VLAN-Tag の付与された EAPOL フレームを受信すると廃棄します。

ポート単位認証の構成例を次の図に示します。

図 6-4 ポート単位認証の構成例

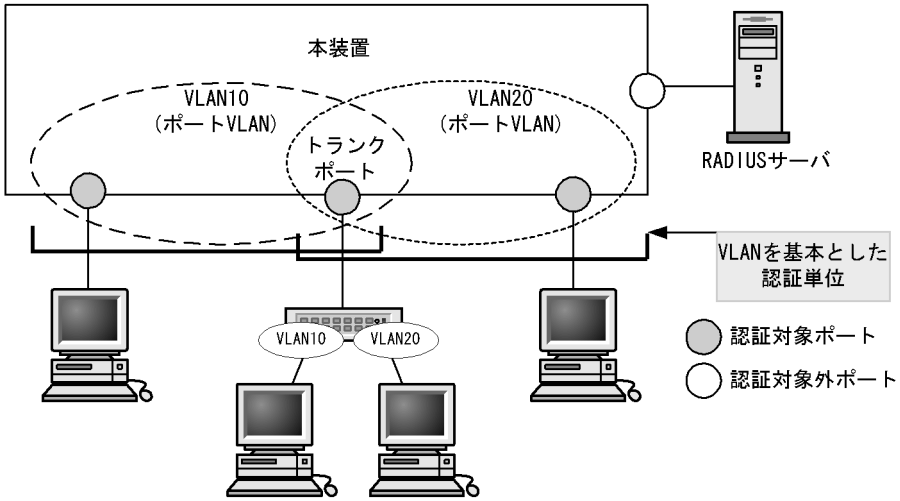


(b) VLAN 単位認証（静的）

認証の制御を VLAN に対して行います。IEEE 802.1Q VLAN-Tag の付与された EAPOL フレームを扱うことができます。端末と本装置の間に L2 スイッチを配置し，L2 スイッチを用いて IEEE 802.1Q VLAN-Tag の付与を行う場合に使用します。Tag の付与されていない EAPOL フレームについては，ポートに設定されているネイティブ VLAN で受信したと認識します。

VLAN 単位認証（静的）の構成例を次の図に示します。

図 6-5 VLAN 単位認証（静的）の構成例



(c) VLAN 単位認証（動的）

認証の制御を MAC VLAN に所属する端末に対して行います。なお，IEEE 802.1Q VLAN-Tag の付与された EAPOL フレームは，この認証モードで扱うことができません。このフレームを受信した場合には，VLAN 単位認証（静的）で扱われます。

指定された MAC VLAN のトランクポートおよびアクセスポートは認証除外ポートとして扱われます。

認証に成功した端末は，認証サーバである RADIUS サーバからの VLAN 情報（MAC VLAN の VLAN ID）に従い，動的に VLAN の切り替えを行います。

VLAN 単位認証（動的）の構成例と動作イメージを次の図に示します。

図 6-6 VLAN 単位認証（動的）の構成例

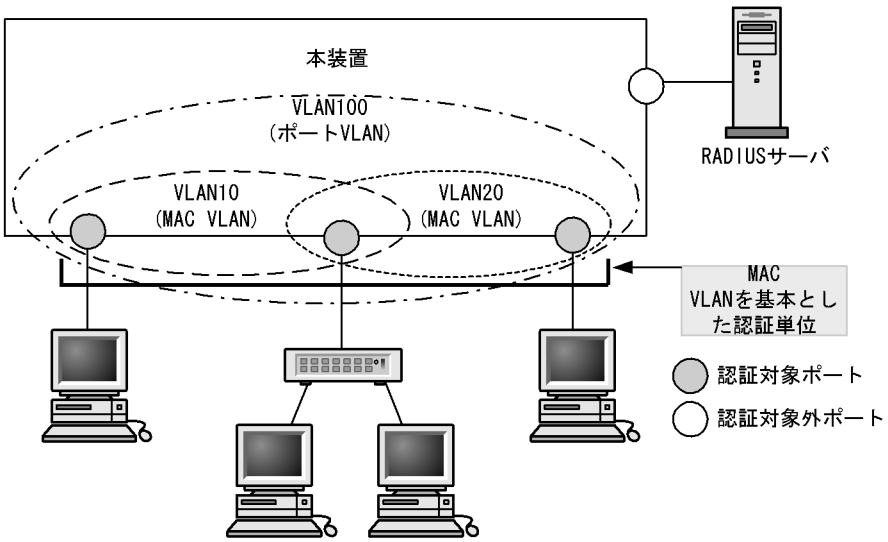
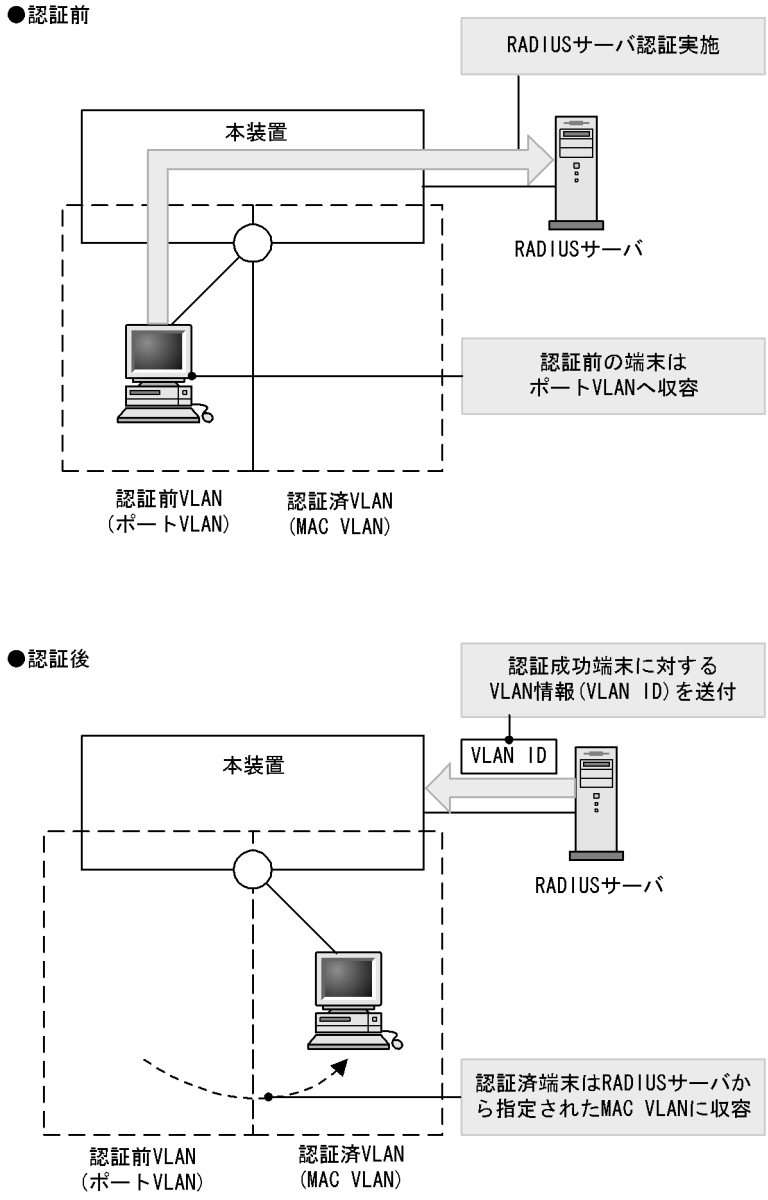


図 6-7 VLAN 単位認証（動的）の動作イメージ



(2) 認証サブモード

基本認証モードに対して設定する認証サブモードを以下に示します。

(a) シングルモード

一つの認証単位内に一つの端末だけ認証して接続するモードです。IEEE802.1X の標準的な認証モードです。最初の端末が認証している状態でほかの端末からの EAP を受信すると，そのポートの認証状態は未認証状態に戻り，コンフィグレーションコマンドで指定された時間が経過したあとに認証シーケンスを再開します。

(b) マルチモード

一つの認証単位内に複数端末の接続を許容しますが，認証対象の端末はあくまで最初に EAP を受信した 1 端末だけのモードです。最初に認証を受けた端末の認証状態に応じて，そのほかの端末のパケットを通信するかどうかが決まります。最初の端末が認証されている状態でほかの端末の EAP を受信すると無視し

ます。

(c) 端末認証モード

一つの認証単位内に複数端末の接続を許容し，端末ごと（送信元 MAC アドレスで識別）に認証を行うモードです。端末が認証されている状態でほかの端末の EAP を受信すると，EAP を送信した端末との間で個別の認証シーケンスが開始されます。

(3) 認証モードオプション

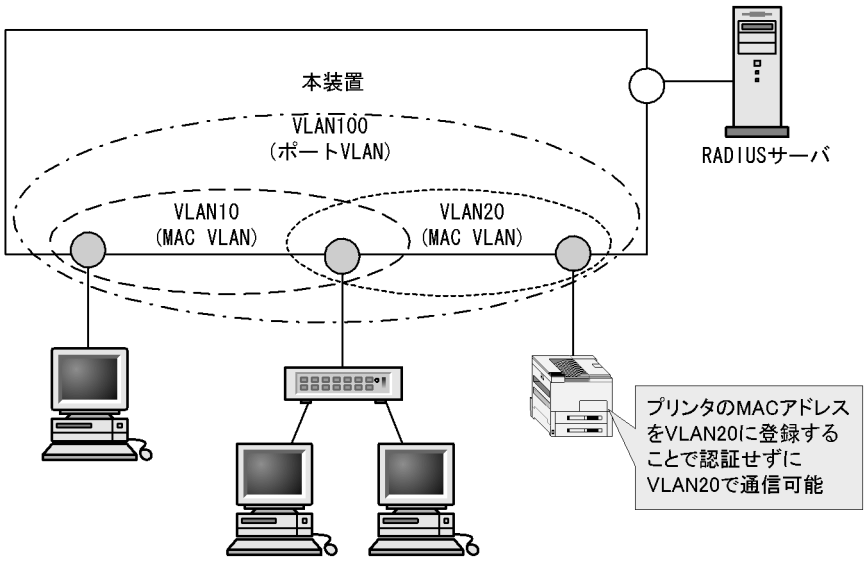
認証モード／認証サブモードに対するオプション設定を以下に示します。

(a) 認証除外端末オプション

スタティック MAC アドレス学習機能および MAC VLAN 機能によって MAC アドレスが設定された端末については認証を不要とし，通信を許可するオプション設定です。Supplicant 機能を持たないプリンタなどの装置やサーバなど認証が不要な端末を，端末単位で認証対象から除外したいときに使用します。端末認証モードの場合だけ使用可能なオプションです。

VLAN 単位認証（動的）での認証除外端末構成例を次の図に示します。

図 6-8 VLAN 単位認証（動的）での認証除外端末構成例



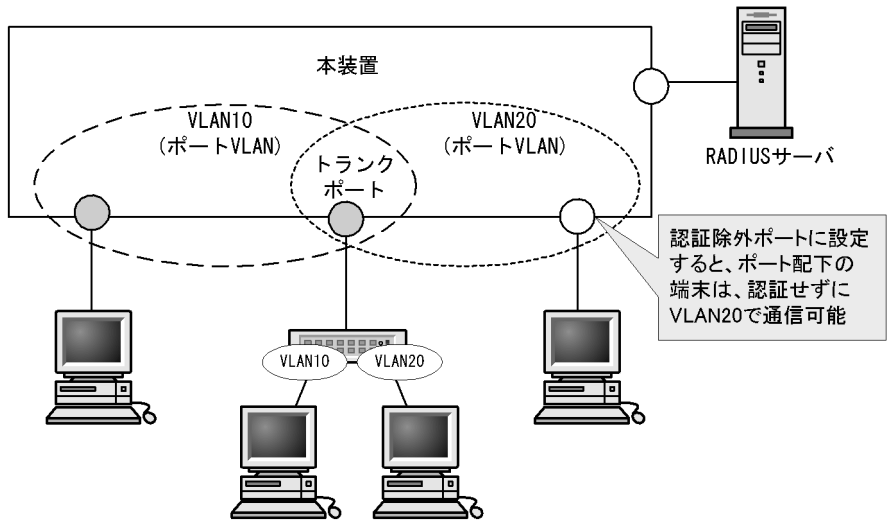
(b) 認証除外ポートオプション

特定の物理ポート番号またはチャネルグループ番号を指定することで，その物理ポートまたはチャネルグループ配下の端末については認証を不要とし，通信を許可するオプション設定です。VLAN 単位認証（静的）の場合だけ使用可能であり，認証対象となる VLAN の中に認証対象外としたいポートがある場合に使用します。

同一ポートに複数の VLAN 単位認証（静的）の VLAN を設定している場合，すべての VLAN で認証除外ポートとなります。

VLAN 単位認証（静的）での認証除外ポート構成例を次の図に示します。

図 6-9 VLAN 単位認証（静的）での認証除外ポート構成例



(c) 認証端末数制限オプション

認証単位内に収容する最大認証端末数を制限するオプション設定です。端末認証モードだけで有効です。認証単位ごとの設定値を次の表に示します。

表 6-10 認証端末数制限オプション

認証モード	初期値	最小値	最大値
ポート単位認証	64	1	64
VLAN 単位認証（静的）	256	1	256
VLAN 単位認証（動的）	256	1	256

(d) 認証デフォルト VLAN 機能

認証デフォルト VLAN 機能は，IEEE802.1X に未対応などの理由によって MAC VLAN に収容できない端末をポート VLAN に収容する機能です。VLAN 単位認証（動的）に設定したポートに対してポート VLAN またはデフォルト VLAN が設定されている場合，その VLAN は認証デフォルト VLAN として動作します。次に示すような場合，端末は認証デフォルト VLAN に収容します。

- IEEE802.1X 未対応の端末
- 認証前の IEEE802.1X 対応の端末
- 認証または再認証に失敗した端末
- RADIUS サーバから指定された VLAN ID が MAC VLAN でない場合

6.2.2 端末検出動作切り替えオプション

端末の認証開始を誘発するために，本装置は tx-period コマンドで指定した間隔で EAP-Request/Identity をマルチキャスト送信します。認証サブモードが端末認証モードの場合，認証単位に複数の端末が存在する可能性があるため，本装置ではすべての端末の認証が完了するまで EAP-Request/Identity の送信を継続することをデフォルトの動作としています。このとき，認証単位当たりの端末数が増えると EAP-Request/Identity に応答した端末の認証処理で装置に負荷を掛けるおそれがあるため，認証済み端末からの応答には認証シーケンスを一部省略することで，装置の負荷を低減しています。

ただし，使用する Supplicant ソフトウェアの種類によっては，認証シーケンスの省略によって認証済み端末の通信が途切れる問題が発生することがあります。そのため，認証済み端末に対する動作を切り替えるオプションを用意しています。本オプションは supplicant-detection コマンドで選択を行い，次に示す四種類の動作を指定できます。

(1) shortcut

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

(2) disable

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

(3) full

認証済み端末に対する EAP-Request/Identity 契機の認証シーケンスを省略しません。本モードは自発的に EAP-Start を送信しない Supplicant ソフトウェアと，認証シーケンスを省略すると問題の発生する Supplicant ソフトウェアを混在して使用する場合に指定してください。本モードを指定した場合は接続できる端末数に制限が発生しますので注意してください。

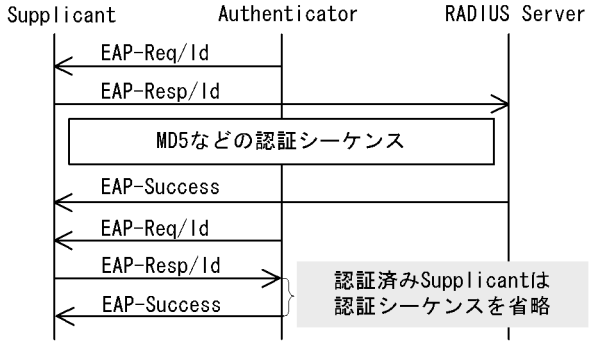
(4) auto

端末検出のための EAP-Request/Identity をマルチキャストアドレスで送信しません。端末が送信した任意のフレームを受信することで認証前の端末を検知して，端末ごとに EAP-Request/Identity をユニキャストアドレスで送信して認証処理を開始します。EAP-Request/Identity をマルチキャストアドレスで送信しないため，認証済み端末に対する EAP-Request/Identity 契機の認証シーケンスは実行されなくなります。

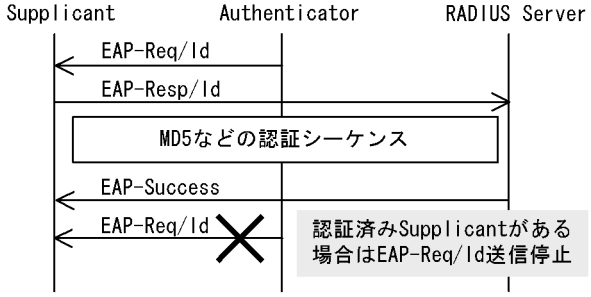
本オプションは端末認証モードだけで有効です。それぞれの動作シーケンスを次の図に示します。

図 6-10 shortcut，disable，full，auto の EAP-Request/Identity のシーケンス

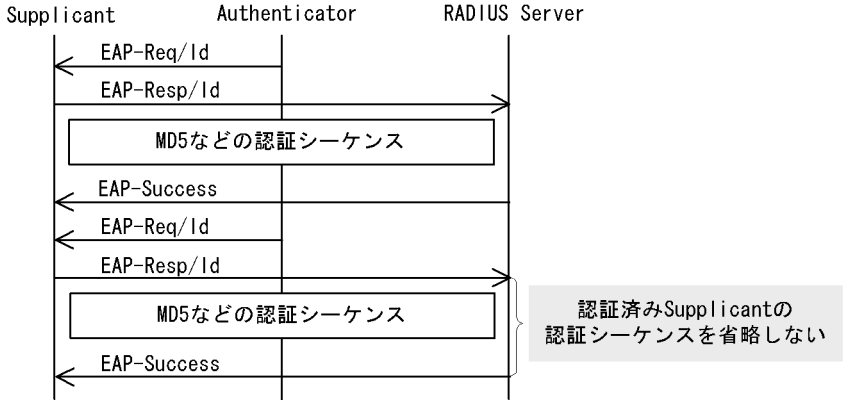
●shortcut指定時のシーケンス（デフォルト）



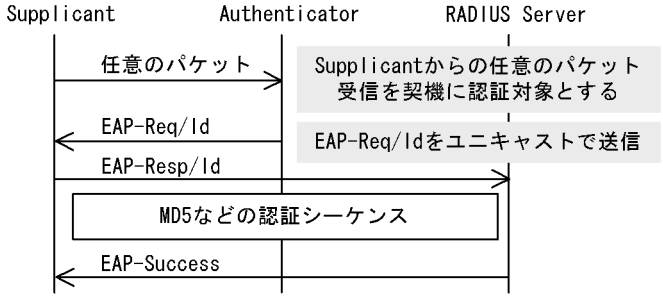
●disable指定時のシーケンス



●full指定時のシーケンス



●auto指定時のシーケンス



6.2.3 端末要求再認証抑止機能

端末から送信される EAPOL-Start を契機とする再認証処理を抑止する機能です。多数の端末から短い間隔で再認証要求が行われるような場合に，再認証処理のために本装置の負荷が上昇するのを防ぎます。本

機能の設定が行われている場合，端末の再認証は本装置がコンフィグレーションで指定した時間間隔で行う定期的な再認証処理で行われます。

6.2.4 RADIUS サーバ接続機能

(1) RADIUS サーバとの接続

RADIUS サーバは最大 4 台まで指定できます。指定時には，サーバの IPv4 アドレス，IPv6 アドレスまたはホスト名を指定できますが，IEEE802.1X では IPv4 アドレスまたは IPv6 アドレスでの指定を推奨します。ホスト名を指定する場合は，「5.4.2 RADIUS サーバ使用時の注意」を参照の上，指定してください。ホスト名を指定したときに複数のアドレスが解決できた場合は，優先順序に従い IP アドレスを一つ決定し，RADIUS サーバと通信を行います。優先順序の詳細については，マニュアル「コンフィグレーションガイド Vol.1 10.1 解説」を参照してください。また，本装置と RADIUS サーバとの接続は，認証の対象外となっているポートを使用してください。

RADIUS サーバへの接続は，コンフィグレーションの順に行い，接続に失敗したときは次の RADIUS サーバとの接続を試みます。すべての RADIUS サーバとの接続に失敗した場合は，端末に EAP-Failure を送信して認証シーケンスを終了します。

RADIUS サーバとの接続後に認証シーケンスの途中で通信タイムアウトを検出した場合は，端末に EAP-Failure を送信し，認証シーケンスを終了します。

(2) VLAN 単位認証（動的）で VLAN を動的に割り当てるときの設定

本装置でサポートする VLAN 単位認証（動的）で VLAN の動的割り当てを実施する場合，RADIUS サーバへ次に示す属性を設定する必要があります。属性の詳細については，「表 6-4 認証で使用する属性名（その 3 Access-Accept）」を参照してください。

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

(3) ポート単位認証の端末認証モード，および VLAN 単位認証（静的）で認証端末にフィルタを適用するときの設定

本装置でサポートするポート単位認証の端末認証モード，および VLAN 単位認証（静的）で認証端末に対してフィルタの適用を実施する場合，RADIUS サーバへ次に示す属性を設定する必要があります。属性の詳細については，「表 6-4 認証で使用する属性名（その 3 Access-Accept）」を参照してください。

- Filter-Id

(4) RADIUS サーバでの本装置の識別の設定

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

- ローカルアドレスが設定されている場合は，ローカルアドレスを送信元 IP アドレスとして使用します。
- ローカルアドレスが設定されていない場合は，送信インタフェースの IP アドレスを送信元 IP アドレスとして使用します。

本装置にローカルアドレスが設定されている場合，RADIUS サーバに登録する本装置の IP アドレスとし

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

6.2.5 EAPOL フォワーディング機能

本装置で IEEE802.1X を動作させない場合に，EAPOL フレームを中継する機能です。EAPOL フレームは宛先 MAC アドレスが IEEE 802.1D で予約されているアドレスであるため通常は中継を行いませんが，IEEE802.1X を使用していない場合はこの機能によって中継が可能です。ほかの Authenticator と端末の間の L2 スイッチとして本装置を使用する場合に設定します。

本機能の設定例は，マニュアル「コンフィグレーションガイド Vol.1　19.6 L2 プロトコルフレーム透過機能のコンフィグレーション」を参照してください。

6.2.6 認証数制限

装置単位およびポート単位に認証数の制限が設定できます。詳細については，「5.3　レイヤ 2 認証共通の機能」を参照してください。

6.2.7 認証済み端末のポート間移動

認証済み端末がポート間移動した場合の取扱いについては，「5.3　レイヤ 2 認証共通の機能」を参照してください。

6.2.8 VLAN 単位認証（動的）の動作モード

VLAN 単位認証（動的）で認証した端末は認証数制限の対象外ですが，VLAN 単位認証（動的）の対象ポートで次に示す設定がある場合，該当ポートで認証した端末は認証数制限の対象となり，同時に認証デフォルト VLAN 機能は動作しなくなります。なお，認証数制限については，「5.3.3　認証数制限」を参照してください。

- Web 認証（ダイナミック VLAN モード）を設定したポート
- MAC 認証を設定したポート
- VLAN 単位認証（静的）の対象 VLAN を dot1q 設定したポート
- 認証専用 IPv4 アクセスリストを設定したポート
- 認証前 ARP パケットリレー機能を設定したポート
- 端末検出動作切り替えオプションを auto に設定した場合（全ポート）

6.2.9 認証端末の疎通制限

ポート単位認証の端末認証モードまたは VLAN 単位認証（静的）では，認証に成功してもフィルタを適用することで疎通制限ができます。設定方法については，「6.2.4　RADIUS サーバ接続機能」を参照してください。

なお，疎通制限された端末は，認証数制限の対象外になります。認証数制限については，「5.3.3　認証数制限」を参照してください。

6.3 IEEE802.1X 使用時の注意事項

(1) 他機能との共存

IEEE802.1X と他機能との共存仕様については，「5.2 レイヤ 2 認証と他機能との共存について」を参照してください。

(2) MAC VLAN をアクセスポートとして指定した場合の注意事項

- MAC VLAN をアクセスポートとして指定したインタフェースにポート単位認証を設定できますが，共存はできませんので使用しないでください。

(3) Interim パケットの送信間隔についての注意事項

RADIUS Accounting の Interim パケットを使用する場合，RADIUS パケットの Acct-Interim-Interval 属性で指定される送信間隔は，600 以上の値を設定することを推奨します。600 より小さい値を設定した場合，全認証済端末数の Interim パケットが送信されるので RADIUS サーバおよびネットワークの負荷が増大するため注意が必要です。

(4) スタティックエントリ登録 MAC と VLAN 単位認証（動的）モードの共存についての注意事項

VLAN 単位認証（動的）を設定している VLAN 内の MAC VLAN モードのインタフェースに対し，mac-address-table static コマンドで MAC アドレステーブルにスタティックエントリが登録されていると，該当する端末は正常に認証処理を行うことができません。

(5) VLAN 単位認証（動的）での MAC アドレス学習のエージング時間設定について

VLAN 単位認証（動的）を使用する場合，指定する MAC VLAN と認証デフォルト VLAN として使用するポート VLAN では，MAC アドレスエントリのエージング時間に 0（無限）を指定しないでください。0（無限）を指定すると，端末の所属する VLAN が切り替わったときに，切り替わる前の VLAN の MAC アドレスエントリがエージングで消去されないで残り続けるため，不要な MAC アドレスエントリが蓄積することになります。切り替わる前の VLAN に不要な MAC アドレスエントリが蓄積した場合は，clear mac-address-table コマンドで消去してください。

(6) タイマ値の変更について

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

(7) 端末と本装置の間に L2 スイッチを配置する場合の注意事項

端末からの応答は一般的にマルチキャストとなるため，端末と本装置の間に L2 スイッチを配置する場合，端末からの応答による EAPOL フレームは L2 スイッチの同一 VLAN の全ポートへ転送されます。したがって，L2 スイッチの VLAN を次のように設定すると，同一端末からの EAPOL フレームが本装置の複数のポートへ届き，複数のポートで同一端末に対する認証処理が行われるようになります。そのため，認証動作が不安定になり，通信が切断されたり，認証ができなくなったりします。

- L2 スイッチの同一 VLAN に設定されているポートを，本装置の認証対象となっている複数のポートに接続した場合

- L2 スイッチの同一 VLAN に設定されているポートを，複数の本装置の認証対象となっているポートに接続した場合

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

図 6-11　禁止構成例

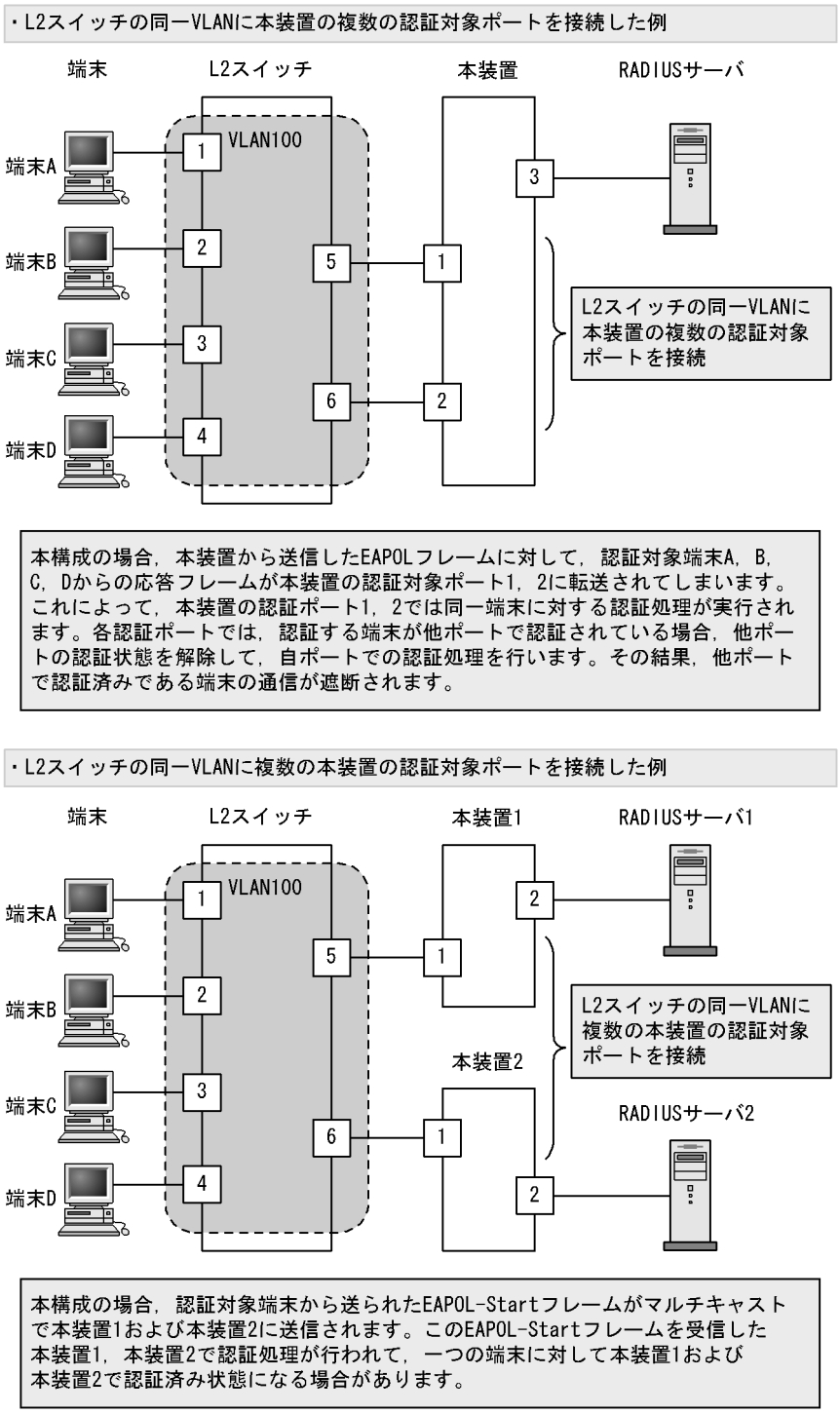
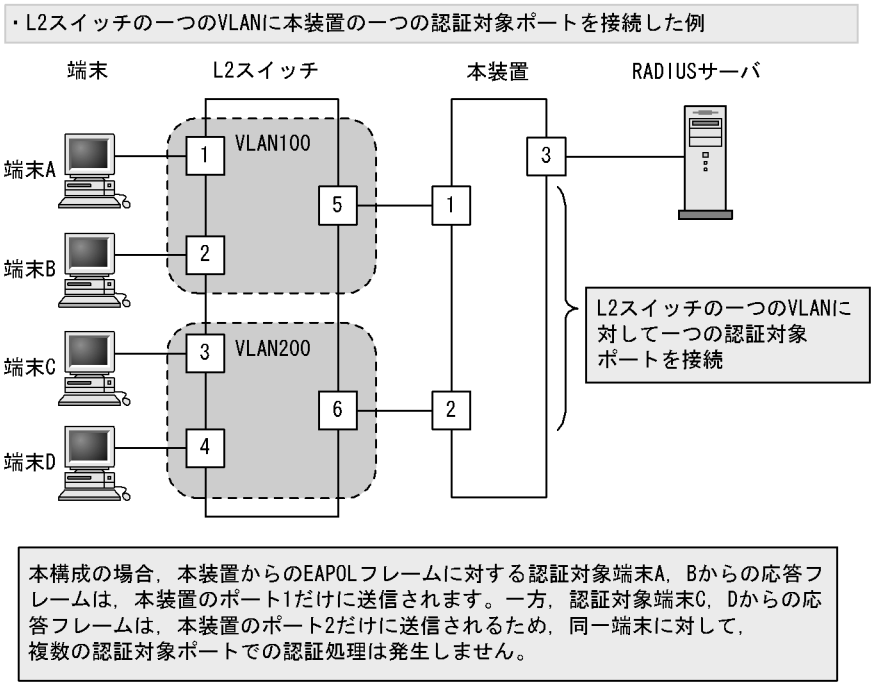


図 6-12 正しい構成例



(8) IEEE802.1X と IP マルチキャストパケットフロー制御補助モードとの共存時の動作

IEEE802.1X と IP マルチキャストパケットフロー制御補助モードを同時に使用して，IEEE802.1X の端末検出動作切り替えオプションを auto に設定した場合，次に示すパケットでの端末検出はしません。

- 宛先アドレスが IPv4 マルチキャストアドレスのパケット
- 宛先アドレスの範囲が ff0::/12 以外の IPv6 マルチキャストパケット
- MLD パケット

7 IEEE802.1X の設定と運用

IEEE802.1X は OSI 階層モデルの第 2 レイヤで認証を行う機能です。この章では，IEEE802.1X のオペレーションについて説明します。

7.1 IEEE802.1X のコンフィグレーション

7.1.1 コンフィグレーションコマンド一覧

IEEE802.1X 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 7-1 コンフィグレーションコマンド一覧

コマンド名	説明
aaa accounting dot1x default	RADIUS サーバでアカウンティング集計を行う場合に設定します。
aaa authentication dot1x default	IEEE802.1X のユーザ認証を RADIUS サーバで行うことを設定します。
aaa authorization network default	RADIUS サーバから指定された VLAN 情報に従って，VLAN 単位認証（動的）を行う場合に設定します。
dot1x force-authorized-port	VLAN 単位認証（静的）で，認証不要で通信を許可するポートまたはチャネルグループを設定します。
dot1x ignore-eapol-start dot1x vlan ignore-eapol-start dot1x vlan dynamic ignore-eapol-start	Supplicant からの EAPOL-Start 受信時に，EAP-Request/Identity を送信しない設定をします。
dot1x logging enable	IEEE802.1X の動作ログに出力する情報を syslog サーバへ出力します。
dot1x loglevel	動作ログメッセージを記録するメッセージレベルを指定します。
dot1x max-req dot1x vlan max-req dot1x vlan dynamic max-req	Supplicant からの応答がない場合に EAP-Request/Identity を再送する最大回数を設定します。
dot1x max-supplicant dot1x vlan max-supplicant dot1x vlan dynamic max-supplicant	認証単位の最大認証端末数を設定します。
dot1x multiple-hosts dot1x multiple-authentication	ポート単位認証の認証サブモードを設定します。
dot1x port-control	ポート単位認証を有効にします。
dot1x reauthentication dot1x vlan reauthentication dot1x vlan dynamic reauthentication	認証済み端末の再認証の有効／無効を設定します。
dot1x supplicant-detection dot1x vlan supplicant-detection dot1x vlan dynamic supplicant-detection	認証サブモードに端末認証モードを指定したときの端末検出動作のオプションを設定します。
dot1x system-auth-control	IEEE802.1X を有効にします。
dot1x timeout keep-unauth	ポート単位認証のシングルモードで，複数の端末からの認証要求を検出したときに，そのポートでの通信遮断状態を保持する時間を設定します。
dot1x timeout quiet-period dot1x vlan timeout quiet-period dot1x vlan dynamic timeout quiet-period	認証（再認証を含む）に失敗した Supplicant の認証処理再開を許可するまでの待機時間を設定します。
dot1x timeout reauth-period dot1x vlan timeout reauth-period dot1x vlan dynamic timeout reauth-period	認証済み端末の再認証を行う間隔を設定します。
dot1x timeout server-timeout dot1x vlan timeout server-timeout dot1x vlan dynamic timeout server-timeout	認証サーバからの応答待ち時間を設定します。

コマンド名	説明
dot1x timeout supp-timeout dot1x vlan timeout supp-timeout dot1x vlan dynamic timeout supp-timeout	Supplicant へ送信した EAP-Request/Identity に対して，Supplicant からの応答待ち時間を設定します。
dot1x timeout tx-period dot1x vlan timeout tx-period dot1x vlan dynamic timeout tx-period	定期的な EAP-Request/Identity の送信間隔を設定します。
dot1x vlan enable	VLAN 単位認証（静的）を有効にします。
dot1x vlan dynamic enable	VLAN 単位認証（動的）を有効にします。
dot1x vlan dynamic radius-vlan	VLAN 単位認証（動的）で，RADIUS サーバからの VLAN 情報により動的な VLAN 割り当てを許可する VLAN を設定します。

7.1.2 IEEE802.1X の基本的な設定

IEEE802.1X の基本認証モード設定について説明します。

(1) IEEE802.1X を有効にする設定

[設定のポイント]

グローバルコンフィグレーションモードで IEEE802.1X を有効にします。このコマンドを実行しないと，IEEE802.1X のほかのコマンドが有効になりません。

[コマンドによる設定]

1. **(config)# dot1x system-auth-control**
   IEEE802.1X を有効にします。

(2) ポート単位認証の設定

物理ポートまたはチャネルグループを認証の対象に設定します。

[設定のポイント]

アクセスポートを設定し，そのポートでポート単位認証を有効にします。認証サブモードを設定します。認証サブモードの設定を省略するとシングルモードになります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport mode access
   ポート 0/1 に access モードを設定します。

2. **(config-if)# dot1x multiple-authentication**
   認証サブモードを端末認証モードに指定します。

3. **(config-if)# dot1x port-control auto**
   ポート単位認証を有効にします。

(3) VLAN 単位認証（静的）の設定

ポート VLAN を認証の対象に設定します。

[設定のポイント]

ポート VLAN を設定し，その VLAN で VLAN 単位認証（静的）を有効にします。

[コマンドによる設定]

1. **(config)# vlan 10**
   (config-vlan)# state active
   (config-vlan)# exit
   VLAN ID 10 にポート VLAN を設定します。

2. **(config)# dot1x vlan 10 enable**
   VLAN ID 10 で VLAN 単位認証（静的）を有効にします。

(4) VLAN 単位認証（動的）の設定

MAC VLAN を認証の対象に設定します。

[設定のポイント]

MAC VLAN を設定し，その VLAN で VLAN 単位認証（動的）を有効にします。
また，VLAN 単位認証（動的）認証に成功した端末を RADIUS サーバから指定された VLAN 情報に従い登録するためには，コンフィグレーションコマンド aaa authorization network default の設定も必要となります。

[コマンドによる設定]

1. **(config)# vlan 100 mac-based**
   (config-vlan)# name MACVLAN100
   (config-vlan)# state active
   (config-vlan)# exit
   VLAN ID 100 に MAC VLAN を設定します。

2. **(config)# dot1x vlan dynamic radius-vlan 100**
   VLAN ID 100 を VLAN 単位認証（動的）の対象に設定します。

3. **(config)# dot1x vlan dynamic enable**
   VLAN 単位認証（動的）を有効にします。

7.1.3 認証モードオプションの設定

認証モードオプションやパラメータの設定について説明します。

(1) 認証除外端末オプションの設定

IEEE802.1X を持たない端末など，認証を行わないで通信を許可する端末の MAC アドレスを設定します。

[設定のポイント]

ポート単位認証，VLAN 単位認証（静的）では，MAC アドレステーブルにスタティックなエントリを登録します。VLAN 単位認証（動的）では，MAC VLAN に MAC アドレスを登録します。

[コマンドによる設定]（ポート単位認証）

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# dot1x multiple-authentication
   (config-if)# dot1x port-control auto
   (config-if)# exit
   ポート 0/1 に VLAN ID 10 を設定し，認証サブモードが端末認証モードのポート単位認証を設定します。

2. **(config)# mac-address-table static 0012.e200.0001 vlan 10 interface gigabitethernet 0/1**
   ポート 0/1 の VLAN ID 10 に認証しないで通信させたい MAC アドレス (0012.e200.0001) をスタティックに設定します。

[コマンドによる設定]（VLAN 単位認証（動的））

1. **(config)# vlan 100 mac-based**
   (config-vlan)# mac-address 0012.e200.0001
   (config-vlan)# exit
   VLAN ID 100 の MAC VLAN で通信可能とする端末の MAC アドレスを設定します。端末は，IEEE802.1X の認証を行わないで VLAN ID 100 で通信できます。

2. **(config)# dot1x vlan dynamic radius-vlan 100**
   (config)# dot1x vlan dynamic enable
   VLAN ID 100 を VLAN 単位認証（動的）の対象に設定して有効にします。

(2) 認証除外ポートオプションの設定

[設定のポイント]

VLAN 単位認証（静的）を設定した VLAN に所属するポートで，認証を行わずに通信を許可するポートを設定します。ポートに複数の VLAN を設定している場合は，すべての VLAN について認証を行わずに通信が可能になります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x force-authorized-port
   VLAN 単位認証（静的）を指定した VLAN に属しているポート 0/1 では認証を行わず，通信できるように設定します。

[注意事項]

認証除外ポートに VLAN 単位認証（静的）を設定した VLAN を追加した場合，そのポートの通信が一度途絶えることがあります。

(3) 認証端末数制限の設定

[設定のポイント]

認証単位ごとに，認証を許可する最大端末数を設定します。ポート単位認証では，認証サブモードに

端末認証モードを設定している場合に有効となります。

［コマンドによる設定］（ポート単位認証）

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x multiple-authentication
   (config-if)# dot1x port-control auto
   (config-if)# dot1x max-supplicant 50
   ポート 0/1 で認証を許可する最大端末数を 50 に設定します。

［コマンドによる設定］（VLAN 単位認証（静的））

1. **(config)# dot1x vlan 10 max-supplicant 50**
   VLAN 単位認証（静的）に設定した VLAN ID 10 で認証を許可する最大端末数を 50 に設定します。

［コマンドによる設定］（VLAN 単位認証（動的））

1. **(config)# dot1x vlan dynamic max-supplicant 50**
   VLAN 単位認証（動的）で認証を許可する最大端末数を 50 に設定します。

（4） 端末検出動作の切替設定

端末の認証開始を誘発するために，本装置は tx-period コマンドで指定した間隔で EAP-Request/Identity をマルチキャスト送信します。このとき，EAP-Request/Identity に応答した認証済み端末に対する認証シーケンス動作を設定します。デフォルトは，認証処理を省略します。

［設定のポイント］

shortcut は，認証処理を省略して本装置の負荷を軽減します。disable は，認証済みの端末が存在する場合には，定期的な EAP-Request/Identity の送信を行いません。full は，認証処理を省略することができない Supplicant を使用している場合に設定します。full モードを指定した場合は，装置の負荷が高くなるので注意が必要です。auto は，EAP-Request/Identity をマルチキャスト送信しません。端末から送信された任意のパケットの受信を契機に，端末ごとに EAP-Request/Identity を送信します。

［コマンドによる設定］（ポート単位認証）

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x multiple-authentication
   (config-if)# dot1x port-control auto
   (config-if)# dot1x supplicant-detection disable
   ポート 0/1 に認証済み端末が存在する場合には EAP-Request/Identity を送信しないように設定します。

［コマンドによる設定］（VLAN 単位認証（静的））

1. **(config)# dot1x vlan 10 supplicant-detection shortcut**
   VLAN 単位認証（静的）に設定した VLAN ID 10 で，認証済み端末からの EAP-Response/Identity 受信では，再認証処理を省略して認証成功とするように設定します。

［コマンドによる設定］（VLAN 単位認証（動的））

1. **(config)# dot1x vlan dynamic supplicant-detection full**
   VLAN 単位認証（動的）で認証済み端末からの EAP-Response/Identity 受信では，認証処理を省略しないで認証サーバへの問い合わせを行います。

7.1.4 認証処理に関する設定

(1) 端末へ再認証を要求する機能の設定

ログオフを送信しないでネットワークから外れた端末は本装置から認証を解除できないため，認証済みの端末に対して再認証を促すことで応答のない端末の認証を解除します。

[設定のポイント]

認証済みの端末ごとに，reauth-period タイマに設定している時間間隔で EAP-Request/Identity を送信します。reauth-period タイマの設定値は，tx-period タイマの設定値よりも大きい値を設定してください。

[コマンドによる設定]（ポート単位認証）

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x reauthentication
   (config-if)# dot1x timeout reauth-period 360
   ポート 0/1 での再認証要求機能を有効に設定し，再認証の時間間隔を 360 秒に設定します。

[コマンドによる設定]（VLAN 単位認証（静的））

1. **(config)# dot1x vlan 10 reauthentication**
   (config)# dot1x vlan 10 timeout reauth-period 360
   VLAN 単位認証（静的）に設定した VLAN ID 10 での再認証機能を有効に設定し，再認証の時間間隔を 360 秒に設定します。

[コマンドによる設定]（VLAN 単位認証（動的））

1. **(config)# dot1x vlan dynamic reauthentication**
   (config)# dot1x vlan dynamic timeout reauth-period 360
   VLAN 単位認証（動的）での再認証機能を有効に設定し，再認証の時間間隔を 360 秒に設定します。

(2) 端末への EAP-Request フレーム再送の設定

端末の認証中に，本装置から送信する EAP-Request（認証サーバからの要求メッセージ）に対して，端末から応答がない場合の再送時間と再送回数を設定します。

[設定のポイント]

再送時間間隔と再送回数の総時間が，reauth-period タイマに設定している時間より短い時間になるように設定してください。

[コマンドによる設定]（ポート単位認証）

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x timeout supp-timeout 60
   ポート 0/1 での EAP-Request フレームの再送時間を 60 秒に設定します。

2. **(config-if)# dot1x max-req 3**
   ポート 0/1 での EAP-Request フレームの再送回数を 3 回に設定します。

[コマンドによる設定]（VLAN 単位認証（静的））

1. **(config)# dot1x vlan 10 timeout supp-timeout 60**
   VLAN 単位認証（静的）に設定した VLAN ID 10 での EAP-Request フレームの再送時間を 60 秒に設定します。

2. **(config)# dot1x vlan 10 max-req 3**
   VLAN 単位認証（静的）に設定した VLAN ID 10 での EAP-Request フレームの再送回数を 3 回に設定します。

[コマンドによる設定]（VLAN 単位認証（動的））

1. **(config)# dot1x vlan dynamic timeout supp-timeout 60**
   VLAN 単位認証（動的）での EAP-Request フレームの再送時間を 60 秒に設定します。

2. **(config)# dot1x vlan dynamic max-req 3**
   VLAN 単位認証（動的）での EAP-Request フレームの再送回数を 3 回に設定します。

(3) 端末からの認証要求を抑止する機能の設定

端末からの EAP-Start フレーム受信による認証処理を抑止します。本機能を設定した場合，新規認証および再認証は，それぞれ tx-period タイマ，reauth-period タイマの時間間隔で行われます。

[設定のポイント]

多数の端末から短い時間間隔で再認証要求が行われ，装置の負荷が高い場合に設定を行い，負荷を低減します。本コマンドの設定前に dot1x reauthentication コマンドの設定が必要です。

[コマンドによる設定]（ポート単位認証）

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x reauthentication
   (config-if)# dot1x ignore-eapol-start
   ポート 0/1 で EAP-Start フレーム受信による認証処理を抑止します。

[コマンドによる設定]（VLAN 単位認証（静的））

1. **(config)# dot1x vlan 10 reauthentication**
   (config)# dot1x vlan 10 ignore-eapol-start
   VLAN 単位認証（静的）に設定した VLAN ID 10 で EAP-Start フレームによる認証処理を抑止します。

[コマンドによる設定]（VLAN 単位認証（動的））

1. **(config)# dot1x vlan dynamic reauthentication**
   (config)# dot1x vlan dynamic ignore-eapol-start

VLAN 単位認証（動的）で EAP-Start フレーム受信による認証処理を抑止します。

(4) 認証失敗時の認証処理再開までの待機時間設定

認証に失敗した端末に対する認証再開までの待機時間を設定します。

[設定のポイント]

認証に失敗した端末から，短い時間に認証の要求が行われることで装置の負荷が高くなることを抑止します。
ユーザが ID やパスワードの入力誤りによって認証が失敗した場合でも，設定した時間を経過しないと認証処理を再開しないので，設定時間には注意してください。

[コマンドによる設定]（ポート単位認証）

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x timeout quiet-period 300
   ポート単位認証を設定しているポート 0/1 に認証処理再開までの待機時間を 300 秒に設定します。

[コマンドによる設定]（VLAN 単位認証（静的））

1. **(config)# dot1x vlan 10 timeout quiet-period 300**
   VLAN 単位認証（静的）を設定している VLAN ID 10 に認証処理再開までの待機時間を 300 秒に設定します。

[コマンドによる設定]（VLAN 単位認証（動的））

1. **(config)# dot1x vlan dynamic timeout quiet-period 300**
   VLAN 単位認証（動的）に認証処理再開までの待機時間を 300 秒に設定します。

(5) EAP-Request/Identity フレーム送信の時間間隔設定

自発的に認証を開始しない端末に対して，認証開始を誘発するために本装置から定期的に EAP-Request/Identity を送信する時間間隔を設定します。

[設定のポイント]

本機能は，tx-period タイマに設定してある時間間隔で EAP-Request/Identity をマルチキャスト送信します。認証済みの端末からも EAP-Response/Identity の応答を受信し，装置の負荷を高くする可能性がありますので，以下の計算式で決定される値を設定してください。

reauth-period ＞ tx-period ≧（装置で認証を行う総端末数÷20）×2

tx-period のデフォルト値が 30 秒であるため，300 台以上の端末で認証を行う場合は，tx-period タイマ値を変更してください。

[コマンドによる設定]（ポート単位認証）

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x timeout tx-period 300
   ポート単位認証を設定しているポート 0/1 に EAP-Request/Identity フレーム送信の時間間隔を 300 秒に設定します。

[コマンドによる設定]（VLAN 単位認証（静的））

1. **(config)# dot1x vlan 10 timeout tx-period 300**
   VLAN 単位認証（静的）を設定している VLAN ID 10 に EAP-Request/Identity フレーム送信の時間間隔を 300 秒に設定します。

[コマンドによる設定]（VLAN 単位認証（動的））

1. **(config)# dot1x vlan dynamic timeout tx-period 300**
   VLAN 単位認証（動的）に EAP-Request/Identity フレーム送信の時間間隔を 300 秒に設定します。

(6) 認証サーバ応答待ち時間のタイマ設定

認証サーバへの要求に対する応答がない場合の待ち時間を設定します。設定した時間が経過すると，Supplicant へ認証失敗を通知します。radius-server コマンドで設定している再送を含めた総時間と比較して短い方の時間で Supplicant へ認証失敗を通知します。

[設定のポイント]

radius-server コマンドで複数のサーバを設定している場合，各サーバの再送回数を含めた総応答待ち時間よりも短い時間を設定すると，認証サーバへ要求している途中で Supplicant へ認証失敗を通知します。設定したすべての認証サーバから応答がないときに認証失敗を通知したい場合は，本コマンドの設定時間の方を長く設定してください。

[コマンドによる設定]（ポート単位認証）

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x timeout server-timeout 300
   ポート単位認証を設定しているポート 0/1 に認証サーバからの応答待ち時間を 300 秒に設定します。

[コマンドによる設定]（VLAN 単位認証（静的））

1. **(config)# dot1x vlan 10 timeout server-timeout 300**
   VLAN 単位認証（静的）を設定している VLAN ID 10 に認証サーバからの応答待ち時間を 300 秒に設定します。

[コマンドによる設定]（VLAN 単位認証（動的））

1. **(config)# dot1x vlan dynamic timeout server-timeout 300**
   VLAN 単位認証（動的）に認証サーバからの応答待ち時間を 300 秒に設定します。

(7) 複数端末からの認証要求時の通信遮断時間の設定

ポート単位認証（シングルモード）が動作しているポートで，複数の端末からの認証要求を検出した場合に，そのポートでの通信を遮断する時間を設定します。

[設定のポイント]

ポートに接続されてはいけない端末を排除するのに必要な時間を設定してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# dot1x timeout keep-unauth 1800
   ポート単位認証を設定しているポート 0/1 に通信遮断状態の時間を 1800 秒に設定します。

(8) syslog サーバへの出力設定

動作ログの syslog サーバへの出力を設定します。

[設定のポイント]

IEEE802.1X の認証情報および動作情報を記録した動作ログを，syslog サーバに出力する設定をします。

[コマンドによる設定]

1. **(config)# dot1x logging enable**
   (config)# logging event-kind aut
   動作ログを syslog サーバに出力する設定をします。

7.1.5 RADIUS サーバ関連の設定

(1) アカウンティングの設定

[設定のポイント]

RADIUS サーバを指定し，アカウンティング集計を行うことを設定します。

[コマンドによる設定]

1. **(config)# aaa accounting dot1x default start-stop group radius**
   RADIUS サーバにアカウンティング集計を行うことを設定します。

(2) RADIUS サーバで認証を行うための設定

[設定のポイント]

ユーザ認証を RADIUS サーバで行うことを設定します。

[コマンドによる設定]

1. **(config)# aaa authentication dot1x default group radius**
   RADIUS サーバでユーザ認証を行うように設定します。

(3) VLAN 単位認証（動的）使用時の設定

[設定のポイント]

VLAN 単位認証（動的）で，認証した端末を RADIUS サーバから指定された VLAN に従って登録することを設定します。

[コマンドによる設定]

1. **(config)# aaa authorization network default group radius**
   RADIUS サーバから指定された VLAN に登録することを設定します。

7.2 IEEE802.1X のオペレーション

7.2.1 運用コマンド一覧

IEEE802.1X の状態を確認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
show dot1x	認証単位ごとの状態や認証済みの Supplicant 情報を表示します。
show dot1x logging	IEEE802.1X プログラムの動作ログメッセージを表示します。
show dot1x statistics	IEEE802.1X 認証にかかわる統計情報を表示します。
clear dot1x auth-state	認証済みの端末情報をクリアします。
clear dot1x logging	IEEE802.1X プログラムの動作ログメッセージをクリアします。
clear dot1x statistics	IEEE802.1X 認証にかかわる統計情報を 0 にクリアします。
reauthenticate dot1x	IEEE802.1X 認証状態を再認証します。
restart dot1x	IEEE802.1X プログラムを再起動します。
dump protocols dot1x	IEEE802.1X プログラムで採取している制御テーブル情報，統計情報をファイルへ出力します。

7.2.2 IEEE802.1X 状態の表示

(1) 認証状態の表示

IEEE802.1X の状態は show dot1x コマンドで確認してください。

(a) 装置全体の状態表示

IEEE802.1X の設定一覧は，show dot1x コマンドを実行して確認してください。

図 7-1 show dot1x コマンドの実行結果

```
> show dot1x
Date 2005/10/20 10:52:40 UTC
System 802.1X : Enable

Port/ChGr/VLAN    AccessControl    PortControl         Status       Supplicants
Port  0/1         ---              Auto                Authorized   1
Port  0/2         Multiple-Hosts   Auto                Unauthorized 0
Port  0/3         Multiple-Auth    Auto                ---          0
ChGr  32          Multiple-Auth    Auto                ---          1
VLAN 10           Multiple-Auth    Auto                ---          1
VLAN 11           Multiple-Auth    Auto                ---          0
VLAN 12           Multiple-Auth    Auto                ---          0
VLAN(Dynamic)     Multiple-Auth    Auto                ---          1
```

(b) ポート単位認証の状態表示

ポート単位認証におけるポートごとの状態情報を show dot1x port コマンドを実行して確認してください。チャネルグループごとの状態は show dot1x channel-group-number コマンドを実行して確認してください。

ポート番号を指定すると，指定したポートの情報を表示します。

detail パラメータを指定すると，認証している端末の情報を表示します。

図 7-2 show dot1x port コマンド（detail パラメータ指定時）の実行結果

```
> show dot1x port 0/1 detail
Date 2005/10/20 10:52:48 UTC
Port  0/1
AccessControl  : ---                        PortControl    : Auto
Status         : Authorized                 Last EAPOL     : 0012.e200.0021
Supplicants    : 1 / 1                      ReAuthMode     : Enable
TxTimer(s)     : 9     / 30                 ReAuthTimer(s): 3585  / 3600
ReAuthSuccess  : 0                          ReAuthFail     : 0
KeepUnauth(s)  : ---   / 3600

 Supplicants MAC     Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
 0012.e200.0021      Authorized     Authenticated  Idle           0
                     15             2005/10/20 10:52:32
```

(c) VLAN 単位認証（静的）の状態表示

VLAN 単位認証（静的）における VLAN ごとの状態は，show dot1x vlan コマンドを実行して確認してください。VLAN ID を指定すると，指定した VLAN の情報を表示します。detail パラメータを指定すると，認証している端末の情報を表示します。

図 7-3 show dot1x vlan コマンド（detail パラメータ指定時）の実行結果

```
> show dot1x vlan 20 detail
Date 2005/10/20 10:52:48 UTC
VLAN 20
AccessControl  : Multiple-Auth              PortControl    : Auto
Status         : ---                        Last EAPOL     : 0012.e200.0003
Supplicants    : 2 / 2 / 256                ReAuthMode     : Enable
TxTimer(s)     : 3518  / 3600               ReAuthTimer(s): 3548  / 3600
ReAuthSuccess  : 0                          ReAuthFail     : 0
SuppDetection  : Shortcut
Port(s): 0/1-10, ChGr  1-5
Force-Authorized Port(s): 0/4,8-10, ChGr  1-5

 Supplicants MAC     Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
 [Port 0/1]
 0012.e200.0003      Authorized     Authenticated  Idle           0
                     84             2005/10/20 10:51:24
 [Port 0/3]
 0012.e200.0004      Authorized     Authenticated  Idle           0
                     5              2005/10/20 10:51:03
```

(d) VLAN 単位認証（動的）の状態表示

VLAN 単位認証（動的）における VLAN ごとの状態は，show dot1x vlan dynamic コマンドを実行して確認してください。VLAN ID を指定すると，指定した VLAN の情報を表示します。detail パラメータを指定すると，認証している端末の情報を表示します。

図 7-4 show dot1x vlan dynamic コマンド（detail パラメータ指定時）の実行結果

```
> show dot1x vlan dynamic detail
Date 2005/10/20 10:52:48 UTC
VLAN(Dynamic)
AccessControl  : Multiple-Auth             PortControl    : Auto
Status         : ---                       Last EAPOL     : 0012.e200.0005
Supplicants    : 1 / 1 / 256               ReAuthMode     : Disable
TxTimer(s)     : 3556  / 3600              ReAuthTimer(s): 3586  / 3600
ReAuthSuccess  : 0                         ReAuthFail     : 0
SuppDetection  : Shortcut
VLAN(s): 20

 Supplicants MAC     Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
 [VLAN 20]           VLAN(Dynamic) Supplicants : 1
 0012.e200.0005      Authorized     Authenticated  Idle           0
                     44             2005/10/20 10:52:03
```

7.2.3 IEEE802.1X 認証状態の変更

(1) 認証状態の初期化

認証状態の初期化を行うには，clear dot1x auth-state コマンドを使用します。ポート番号，VLAN ID，端末の MAC アドレスのどれかを指定できます。何も指定しなかった場合は，すべての認証状態を初期化します。

コマンドを実行した場合，再認証を行うまで通信ができなくなるので注意してください。

図 7-5 装置内すべての IEEE802.1X 認証状態を初期化する実行例

```
> clear dot1x auth-state
Initialize all 802.1X Authentication Information. Are you sure? (y/n) :y
```

(2) 強制的な再認証

強制的に再認証を行うには，reauthenticate dot1x コマンドを使用します。ポート番号，VLAN ID，端末の MAC アドレスのどれかを指定できます。指定がない場合は，すべての認証済み端末に対して再認証を行います。

コマンドを実行しても，再認証に成功した Supplicant の通信に影響はありません。

図 7-6 装置内すべての IEEE802.1X 認証ポート，VLAN で再認証する実行例

```
> reauthenticate dot1x
Reauthenticate all 802.1X ports and vlans. Are you sure? (y/n) :y
```

8 Web 認証の解説

Web 認証は，汎用 Web ブラウザを用いて認証されたユーザ単位に VLAN へのアクセス制御を行う機能です。この章では Web 認証について解説します。

8.1 概要

Web 認証は，Internet Explorer などの汎用の Web ブラウザ（以降，単に Web ブラウザと表記）を利用しユーザ ID およびパスワードを使った認証によってユーザを認証します。本装置は，認証に成功したユーザが使用する端末の MAC アドレスを使用して認証後のネットワークへのアクセスを可能にします。

この機能によって，端末側に特別なソフトウェアをインストールすることなく，Web ブラウザだけで認証ができます。

(1) 認証モード

本装置は次に示す認証モードをサポートしています。

- 固定 VLAN モード
  端末が認証に成功したあと，MAC アドレスを MAC アドレステーブルに登録して，VLAN 内へ通信できるようにします。端末が認証ネットワークへログインする方法として，本装置の URL リダイレクト機能を使用する方法と Web 認証専用 IP アドレスを使用する方法があります。
- ダイナミック VLAN モード
  端末が認証に成功したあと，MAC アドレスを MAC VLAN と MAC アドレステーブルに登録して，認証前のネットワークと認証後のネットワークを分離します。端末が認証ネットワークへログインする方法として，本装置の URL リダイレクト機能を使用する方法と Web 認証専用 IP アドレスを使用する方法があります。
- レガシーモード
  端末が認証に成功したあと，MAC アドレスを MAC VLAN に登録して，認証前のネットワークと認証後のネットワークを分離します。端末は，ダイナミック VLAN モードと異なり，認証前の VLAN インタフェースの IP アドレスで本装置にログインします（このモードは，Ver.10.6 までのダイナミック VLAN モードです）。

ダイナミック VLAN モードおよびレガシーモードの記述で，認証前の端末が所属する VLAN を認証前 VLAN と呼びます。また，認証後の VLAN を認証後 VLAN と呼びます。

(2) 認証方式

本装置は固定 VLAN モード，ダイナミック VLAN モードおよびレガシーモードのどの認証モードでも，次に示すローカル認証方式または RADIUS 認証方式のどちらかの方式を選択できます。

- ローカル認証方式
  本装置に内蔵した認証用 DB（**内蔵 Web 認証 DB** と呼びます）にユーザ情報を登録しておき，PC から入力された情報との一致を確認して認証する方式です。ネットワーク内に RADIUS サーバを置かない小規模ネットワークに適しています。
- RADIUS 認証方式
  ネットワーク内に設置した RADIUS サーバを用いて認証する方式です。比較的規模の大きなネットワークに適しています。

(3) 認証ネットワーク

本装置の Web 認証は，IPv4 ネットワークを認証対象とします。したがって，認証の対象となる端末を収容する VLAN インタフェースには，IPv4 アドレスを設定する必要があります。ただし，RADIUS サーバの設定では，IPv4 アドレスまたは IPv6 アドレスのどちらでも指定できます。

8.2 システム構成例

ここでは，固定 VLAN モード，ダイナミック VLAN モードおよびレガシーモードの各認証モードについて，ローカル認証方式および RADIUS 認証方式の場合のシステム構成を示します。

また，認証対象の端末への IP アドレス設定方法の違いによるネットワーク構成例を示します。

8.2.1 固定 VLAN モード

固定 VLAN モードでは，認証対象端末が認証前のときは，MAC アドレステーブルに登録されず，接続された VLAN 内へ通信できない状態です。認証が成功すると，端末の MAC アドレスを MAC アドレステーブルに登録し，VLAN 内へ通信できるようになります。

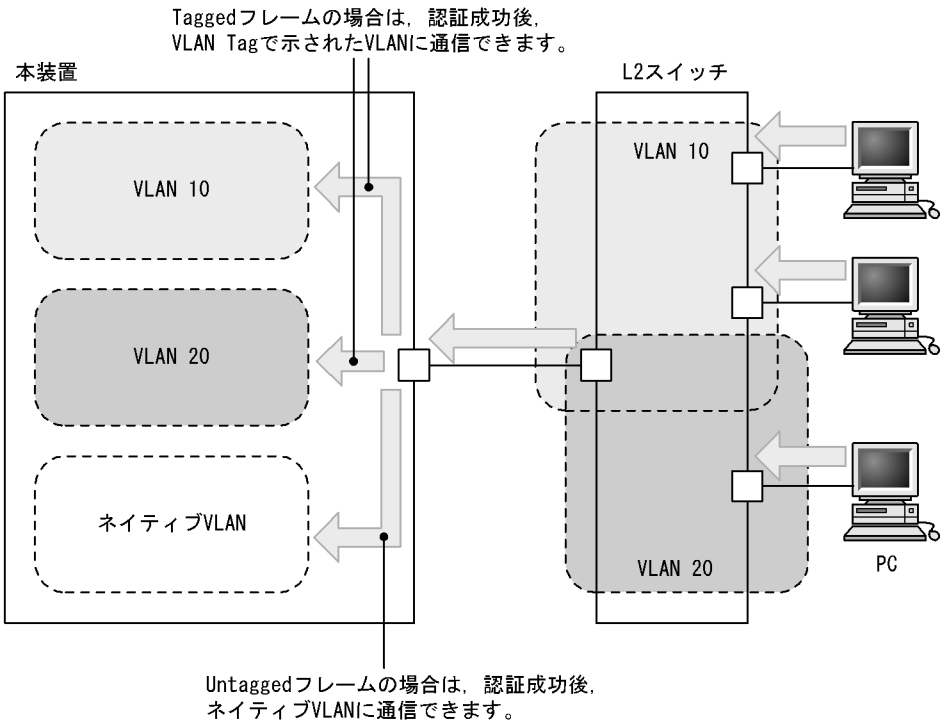
本装置では認証ポートとして次のポートを設定できます。

- アクセスポート
- トランクポート

トランクポートに入ってきた Tagged フレームおよび Untagged フレームの扱いを次に示します。

- 認証時のパケットが Tagged フレームの場合，認証成功後は VLAN Tag で示された VLAN に通信できます。
- 認証時のパケットが Untagged フレームの場合，認証成功後はネイティブ VLAN に通信できます。

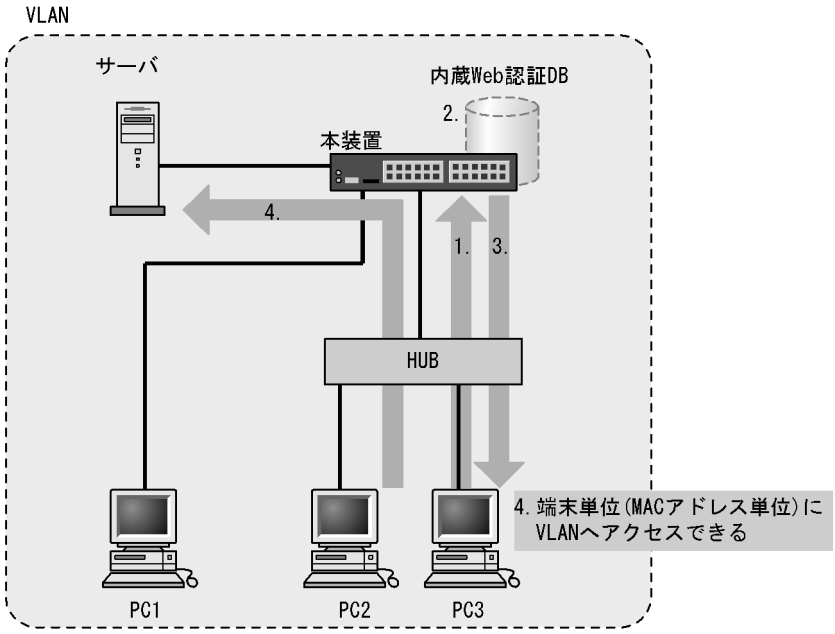
図 8-1 トランクポートの扱い



(1) ローカル認証方式

内蔵 Web 認証 DB を使用したローカル認証方式の構成を次の図に示します。

図 8-2 固定 VLAN モード時のローカル認証方式の構成

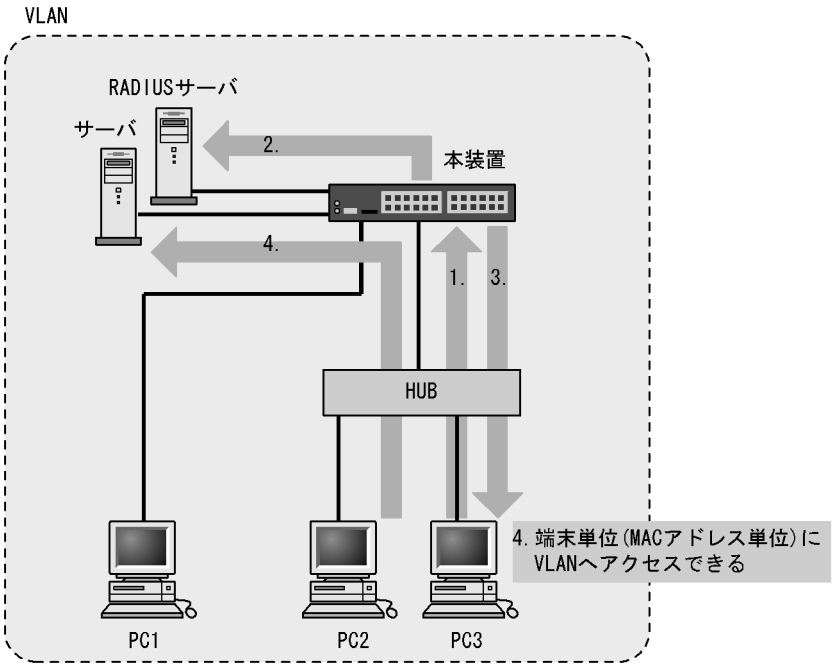


1. HUB 経由で接続された PC から Web ブラウザを起動し，本装置にアクセスします。
2. 本装置の内蔵 Web 認証 DB に登録されたユーザ情報と，PC から入力されたユーザ ID およびパスワードとの一致を確認する認証を行います。
3. 認証が成功であれば，認証成功画面を PC に表示します。
4. 認証済み PC は接続された VLAN のサーバに接続できるようになります。

(2) RADIUS 認証方式

RADIUS サーバを使用した RADIUS 認証方式の構成を次の図に示します。

図 8-3 固定 VLAN モード時の RADIUS 認証方式の構成



1. HUB 経由で接続された PC から Web ブラウザを起動し，本装置にアクセスします。
2. RADIUS サーバに登録されたユーザ情報と，PC から入力されたユーザ ID およびパスワードとの一致を確認する認証を行います。
3. 認証が成功であれば，認証成功画面を PC に表示します。
4. 認証済み PC は接続された VLAN のサーバに接続できるようになります。

8.2.2 ダイナミック VLAN モード

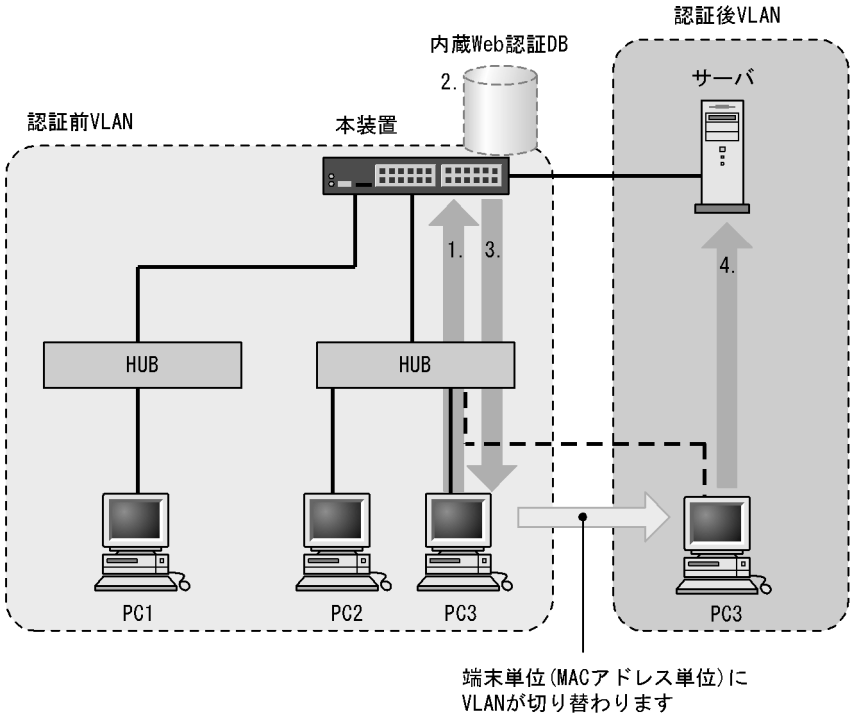
ダイナミック VLAN モードでは，認証前 VLAN に収容されていた端末を，認証成功後，内蔵 Web 認証 DB または RADIUS に登録されている VLAN ID を使用して，MAC VLAN と MAC アドレステーブルに登録して認証後 VLAN への通信を許可します。このため，次に示す設定が必要になります。

- MAC VLAN が設定されているポートを認証ポートとして設定

(1) ローカル認証方式

内蔵 Web 認証 DB を使用したローカル認証方式の構成を次の図に示します。

図 8-4 ダイナミック VLAN モードのローカル認証方式の構成

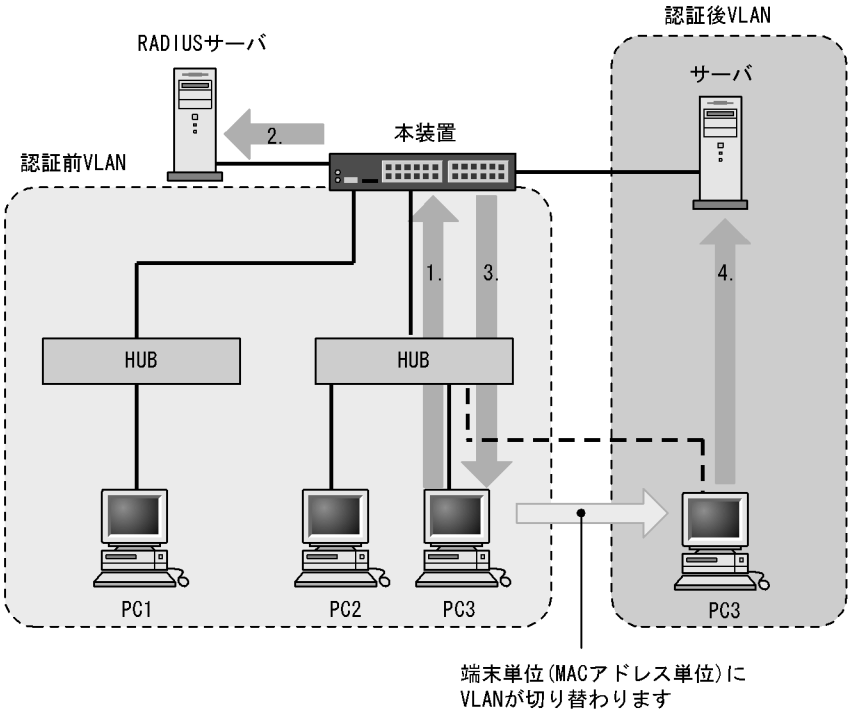


1. HUB 経由で接続された PC から Web ブラウザを起動し，本装置にアクセスします。
2. 本装置の内蔵 Web 認証 DB に登録されたユーザ情報と，PC から入力されたユーザ ID およびパスワードとの一致を確認する認証を行います。
3. 認証が成功であれば，認証成功画面を PC に表示し，認証後 VLAN へ切り替わります。
4. 認証済みの PC は，認証後 VLAN のサーバに接続できるようになります。

(2) RADIUS 認証方式

RADIUS サーバを使用した RADIUS 認証方式の構成を次の図に示します。

図 8-5 ダイナミック VLAN モードの RADIUS 認証方式の構成



1. HUB 経由で接続された PC から Web ブラウザを起動し，本装置にアクセスします。
2. RADIUS サーバに登録されたユーザ情報と，PC から入力されたユーザ ID およびパスワードとの一致を確認する認証を行います。
3. 認証が成功であれば，認証成功画面を PC に表示し，認証後 VLAN へ切り替わります。
4. 認証済みの PC は，認証後 VLAN のサーバに接続できるようになります。

8.2.3 レガシーモード

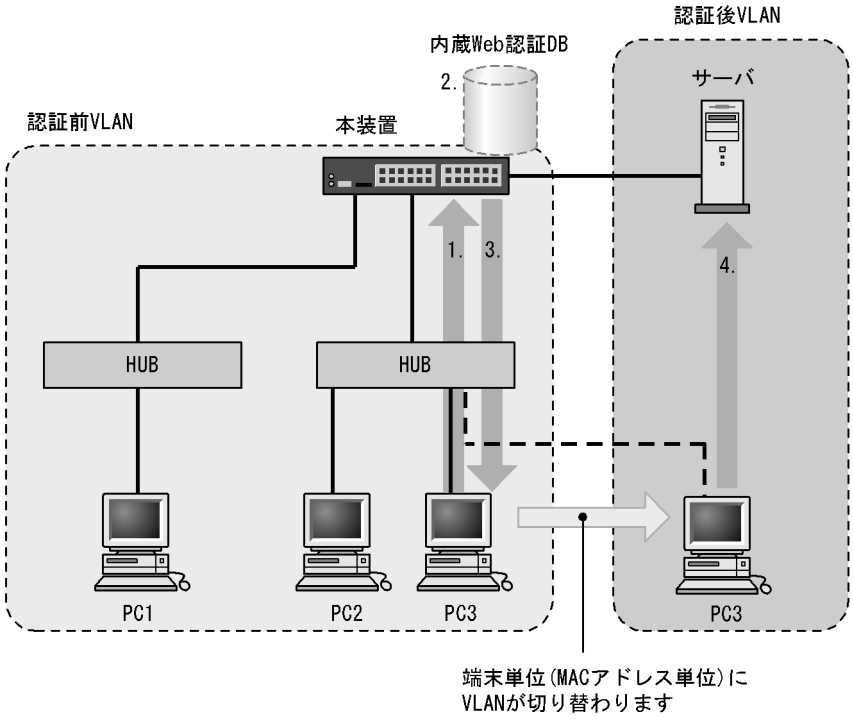
このモードでは，認証前 VLAN をネイティブ VLAN に，認証後 VLAN を MAC VLAN として設定しておきます。認証対象端末が認証前は，端末の MAC アドレスを認証前 VLAN に収容していますが，認証が成功すると，認証後 VLAN に収容します。このため，次に示す設定が必要になります。

- 認証後に切り替わる VLAN の設定

(1) ローカル認証方式

内蔵 Web 認証 DB を使用したローカル認証方式の構成を次の図に示します。

図 8-6 Web 認証システム構成図（ローカル認証方式）

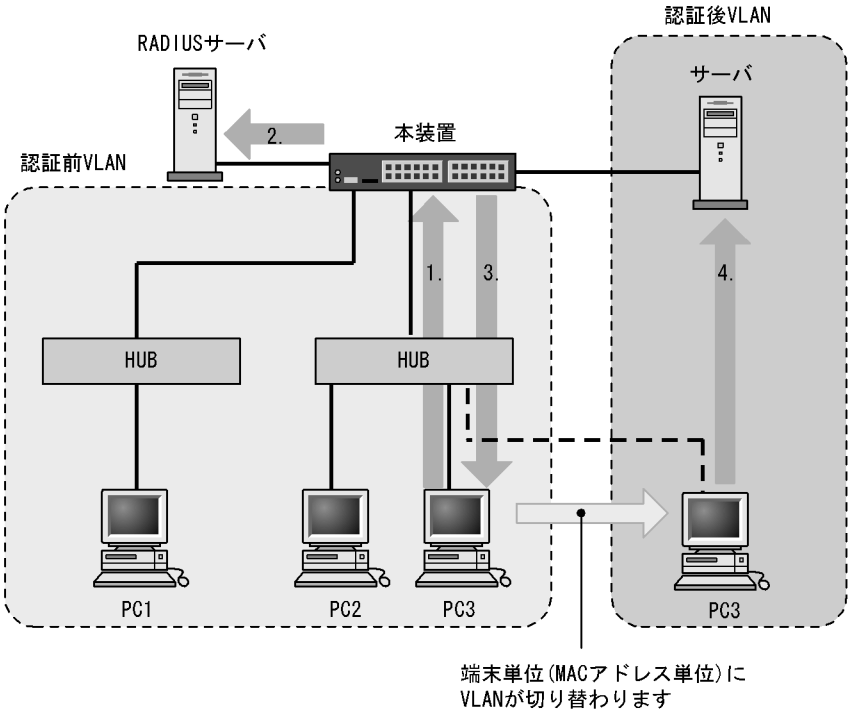


1. HUB 経由で接続された PC から Web ブラウザを起動し，本装置にアクセスします。
2. 本装置の内蔵 Web 認証 DB に登録されたユーザ情報と，PC から入力されたユーザ ID およびパスワードとの一致を確認する認証を行います。
3. 認証が成功であれば，認証成功画面を PC に表示し，認証後 VLAN へ切り替わります。
4. 認証済みの PC は，認証後 VLAN のサーバに接続できるようになります。

(2) RADIUS 認証方式

RADIUS サーバを使用した RADIUS 認証方式の構成を次の図に示します。

図 8-7 Web 認証システム構成図（RADIUS 認証方式）



1. HUB 経由で接続された PC から Web ブラウザを起動し，本装置にアクセスします。
2. RADIUS サーバに登録されたユーザ情報と，PC から入力されたユーザ ID およびパスワードとの一致を確認する認証を行います。
3. 認証が成功であれば，認証成功画面を PC に表示し，認証後 VLAN へ切り替わります。
4. 認証済みの PC は，認証後 VLAN のサーバに接続できるようになります。

8.2.4 IP アドレス設定方法による構成例

Web 認証の対象となる端末に IP アドレスを設定する方法には次の三つがあります。Web 認証は IPv4 ネットワークを対象とするため，ここで説明する IP アドレスは IPv4 アドレスです。

- 本装置内蔵の DHCP サーバ機能で IP アドレスを配布する
- 外部 DHCP サーバを使用する
- 手動で端末の IP アドレスを設定する

固定 VLAN モードでは，認証の前後で端末の IP アドレスを変更する必要はありません。一方，ダイナミック VLAN モードおよびレガシーモードでは，認証の前後で端末が収容される VLAN の変更に伴い IP サブネットも変更されるため，IP アドレスを変更する必要があります。

次に，ダイナミック VLAN モードおよびレガシーモードでの IP アドレス設定方法ごとにシステム構成例を示します。

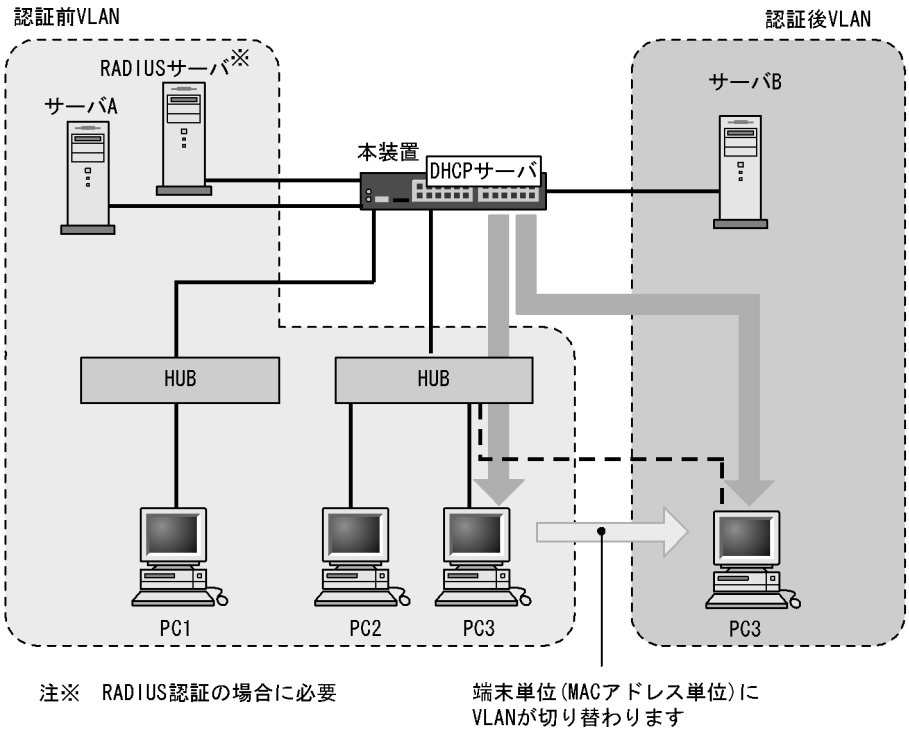
(1) 本装置内蔵の DHCP サーバ機能で IP アドレスを配布する場合

本装置に実装している DHCP サーバを用意する際の構成例を次の図に示します。

認証端末に対して，DHCP サーバ機能から，認証前 VLAN の IP アドレスが配布されたあと，Web ブラウザを用いて認証を行います。

認証が完了すると端末は，認証後 VLAN に切り替わります。VLAN が切り替わり，端末の IP アドレスリースタイムアウト後に，DHCP サーバから認証後 VLAN の IP アドレスが配布され，端末からアクセスできるようになります。

図 8-8　Web 認証システム構成図（内蔵 DHCP サーバ使用）



注意

- DHCP サーバに，認証前 VLAN 用の IP アドレス配布設定と，認証後 VLAN 用の IP アドレス配布設定とを行う必要があります。
- DHCP サーバに，デフォルトゲートウェイアドレスを端末に配布するための設定が必要です。

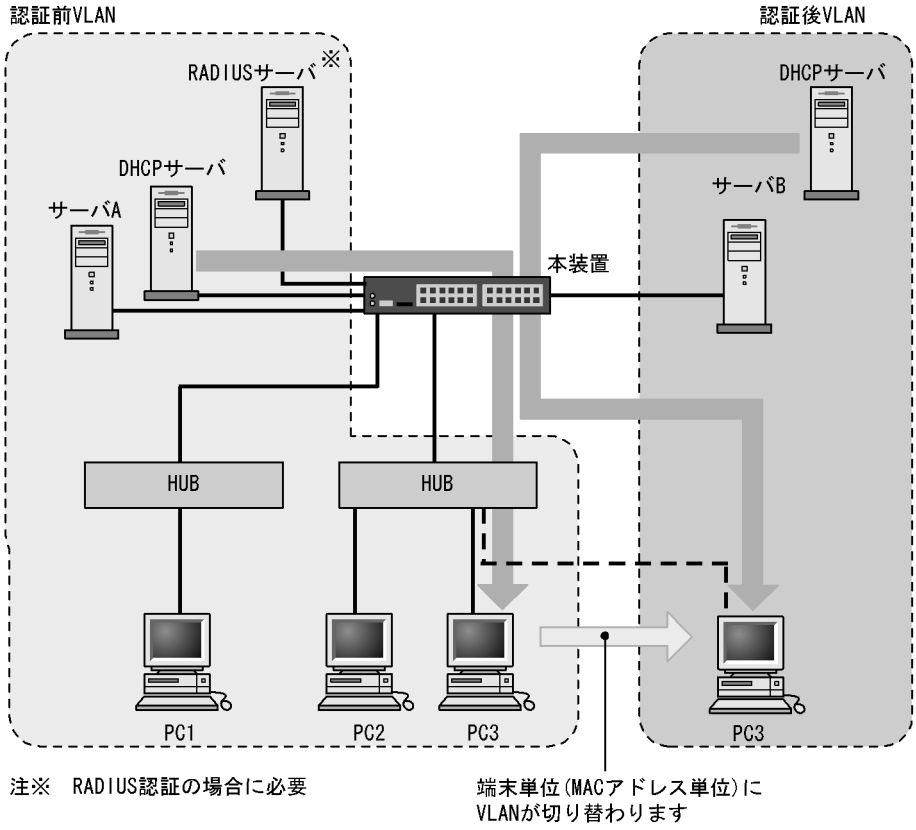
(2) 外部 DHCP サーバを使用する場合

端末認証する際に使用する IP アドレスの配布および認証後の IP アドレス配布を外部 DHCP サーバから行う場合の構成例を次の図に示します。

認証端末には外部 DHCP サーバから，認証前 VLAN の IP アドレスが配布されたあと Web ブラウザによって認証を行います。

認証が完了すると端末は，認証後 VLAN に切り替わります。端末の IP アドレスリースタイムアウト後に，外部 DHCP サーバから認証後 VLAN の IP アドレスが配布されます。

図 8-9　Web 認証システム構成図（外部 DHCP サーバ）



注意

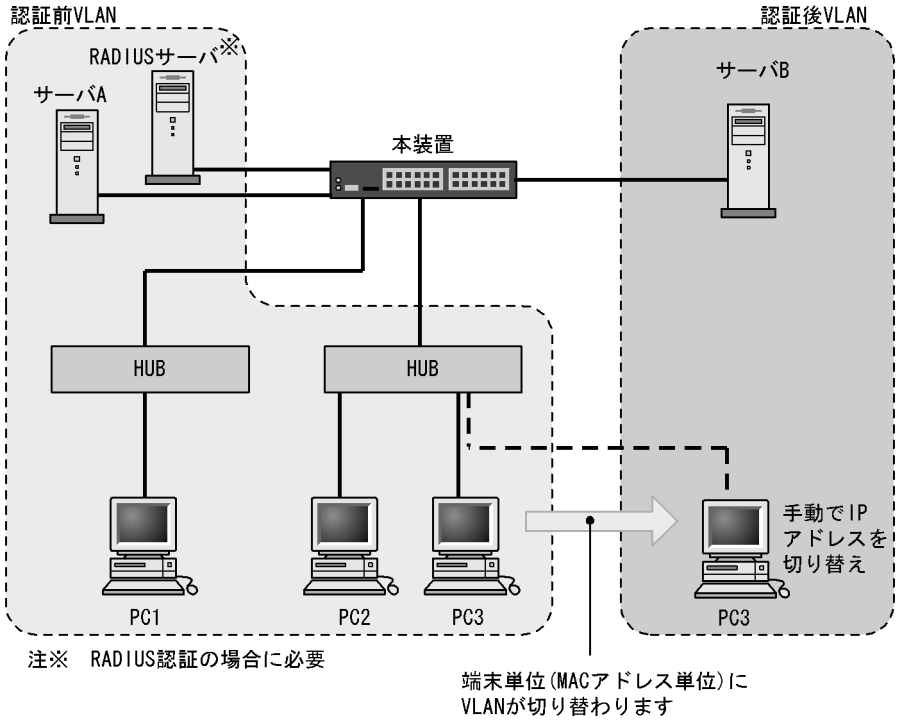
- 外部 DHCP サーバに，デフォルトゲートウェイアドレスを端末に配布するための設定が必要です。

(3) 手動で端末の IP アドレスを設定する場合

認証対象端末の IP アドレスを，認証完了後に手動で設定変更する場合の構成例を次の図に示します。

認証前 VLAN に接続された端末は，認証後に手動で IP アドレスを認証後 VLAN のサブネットの属する IP アドレスに変更することによって認証後 VLAN へのアクセスが可能となります。

図 8-10 Web 認証システム構成図（手動 IP アドレス切り替え）



注意

- 認証後に誤った IP アドレスを設定した場合，認証が成功であってもネットワークにアクセスできなくなります。

8.3 認証機能

8.3.1 認証前端末の通信許可

認証前端末の通信を許可するには認証専用 IPv4 アクセスリストの設定が必要です。認証専用 IPv4 アクセスリストについては「5.3 レイヤ 2 認証共通の機能」を参照してください。

8.3.2 認証ネットワークへのログイン

固定 VLAN モードおよびダイナミック VLAN モードでは，認証前の端末が認証ネットワークへログインする方法として，URL リダイレクト機能を使用する方法と Web 認証専用 IP アドレスを使用する方法があります。どちらの方法も，Web 認証専用 IP アドレスの設定が必要です。

Web 認証専用 IP アドレスは，Web 認証で使用する，端末から本装置へのアクセス専用の IPv4 アドレスです。このアドレスは装置のインタフェースに付けられたアドレスとは異なるため，異なる IP サブネットに収容される端末から認証ネットワークへのログイン操作およびログアウト操作を，すべて同じ IP アドレスで実施できます。また，Web 認証専用 IP アドレスは装置外には送出しないので，ネットワーク内の複数の本装置に同じアドレスを設定できます。したがって，どの端末からも同じ操作で認証ネットワークへのログインおよびログアウトができます。

注意

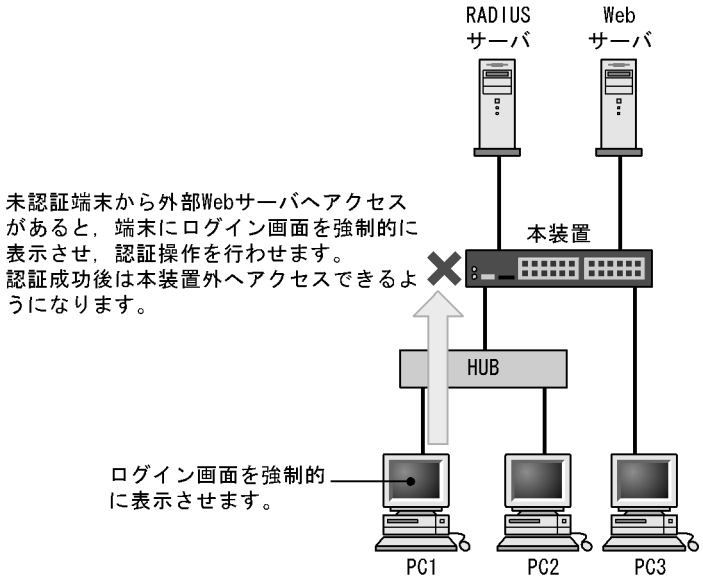
- Web 認証専用 IP アドレスを使用する場合 , コンフィグレーションコマンド authentication arp-relay を設定する必要があります。設定されていない場合は，端末のデフォルトゲートウェイの設定で本装置のインタフェースの IP アドレスを指定してください。

(1) URL リダイレクト機能

認証前の端末が認証ネットワークへログインする場合に，認証前の端末から装置外の Web サーバ宛ての http または https アクセスを検出し，端末の画面に強制的にログイン画面を表示してログイン操作をさせることができます。

また，コンフィグレーションコマンド web-authentication ip address で FQDN（Fully Qualified Domain Name）を指定すれば，リダイレクト先 URL として使用できます。

図 8-11 URL リダイレクト機能



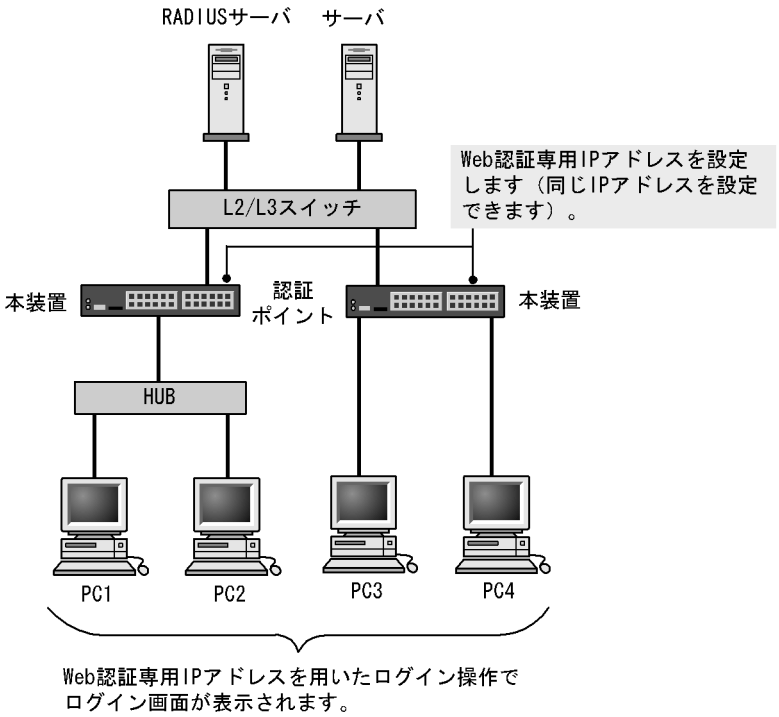
注意

- 端末の Web ブラウザにプロキシサーバを設定した状態で，次のどちらかの方法で URL リダイレクトを使用する場合は，必ず Web 認証専用 IP アドレスがプロキシサーバの適用を受けないように設定してください。
  ・コンフィグレーションコマンド web-authentication redirect-mode で，https パラメータを設定
  ・認証前状態の端末から https でアクセス
- 本機能を使用して，認証前の端末から https で URL アクセスを行ったとき，装置に登録された証明書のドメイン名と一致していない場合，証明書不一致の警告メッセージが Web ブラウザ上に表示されます。なお，警告メッセージが表示されても，続行する操作を行うと，Web 認証のログイン画面が表示されてログイン操作が行えます。

(2) Web 認証専用 IP アドレスによるログイン操作

本装置に設定された Web 認証専用の IP アドレスを使用してログイン操作，およびログアウト操作ができます。

図 8-12 Web 認証専用 IP アドレスによるログイン操作



8.3.3 ワンタイムパスワード認証【OP-OTP】

本装置では，RSA 社の RSA SecurID と連携したワンタイムパスワード認証機能を提供します。なお，本機能を使用する場合は，オプションライセンス OP-OTP の設定が必要です。

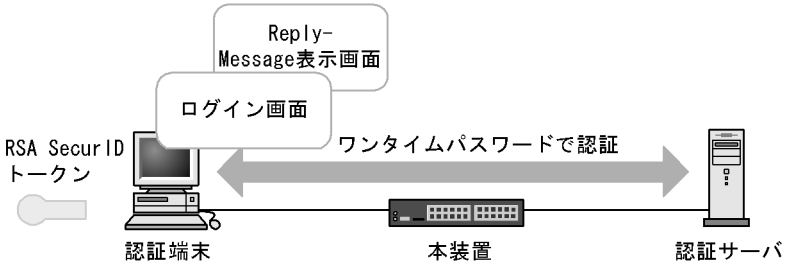
ワンタイムパスワード認証では，ユーザ ID とパスワードによる認証ではなく，次の三つの情報を使用して認証操作をします。

- ユーザ ID
- ユーザが所持している PIN コード（ユーザが独自に設定できるコード）
- トークンと呼ばれる機構（ハードウェアトークンとソフトウェアトークンがある）で生成したトークンコード（ワンタイムパスワード）

なお，PIN コードは，認証サーバから送られてくるメッセージを表示した Reply-Message 表示画面で入力します。

ワンタイムパスワード認証の構成を次の図に示します。

図 8-13 ワンタイムパスワード認証の構成

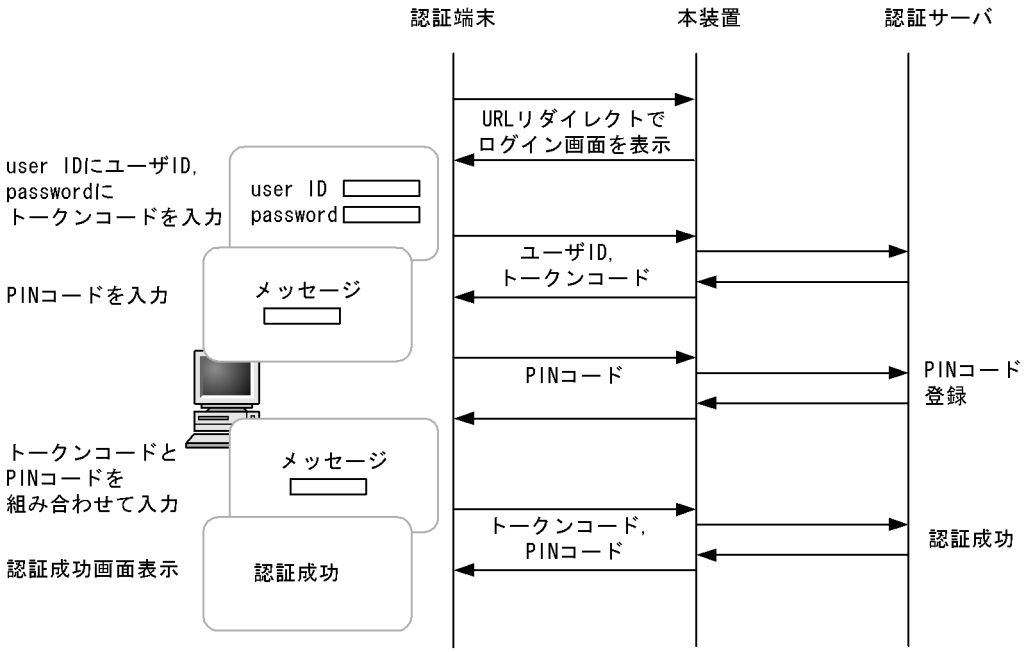


本装置では，New PIN モードと Next Token モードをサポートします。なお，本機能は，固定 VLAN モードとダイナミック VLAN モードで動作します。

（1） New PIN モード

認証サーバに事前に PIN コードを登録しないで，最初にログイン操作をしたときに PIN コードを登録するモードです。New PIN モードでの動作概要を次の図に示します。

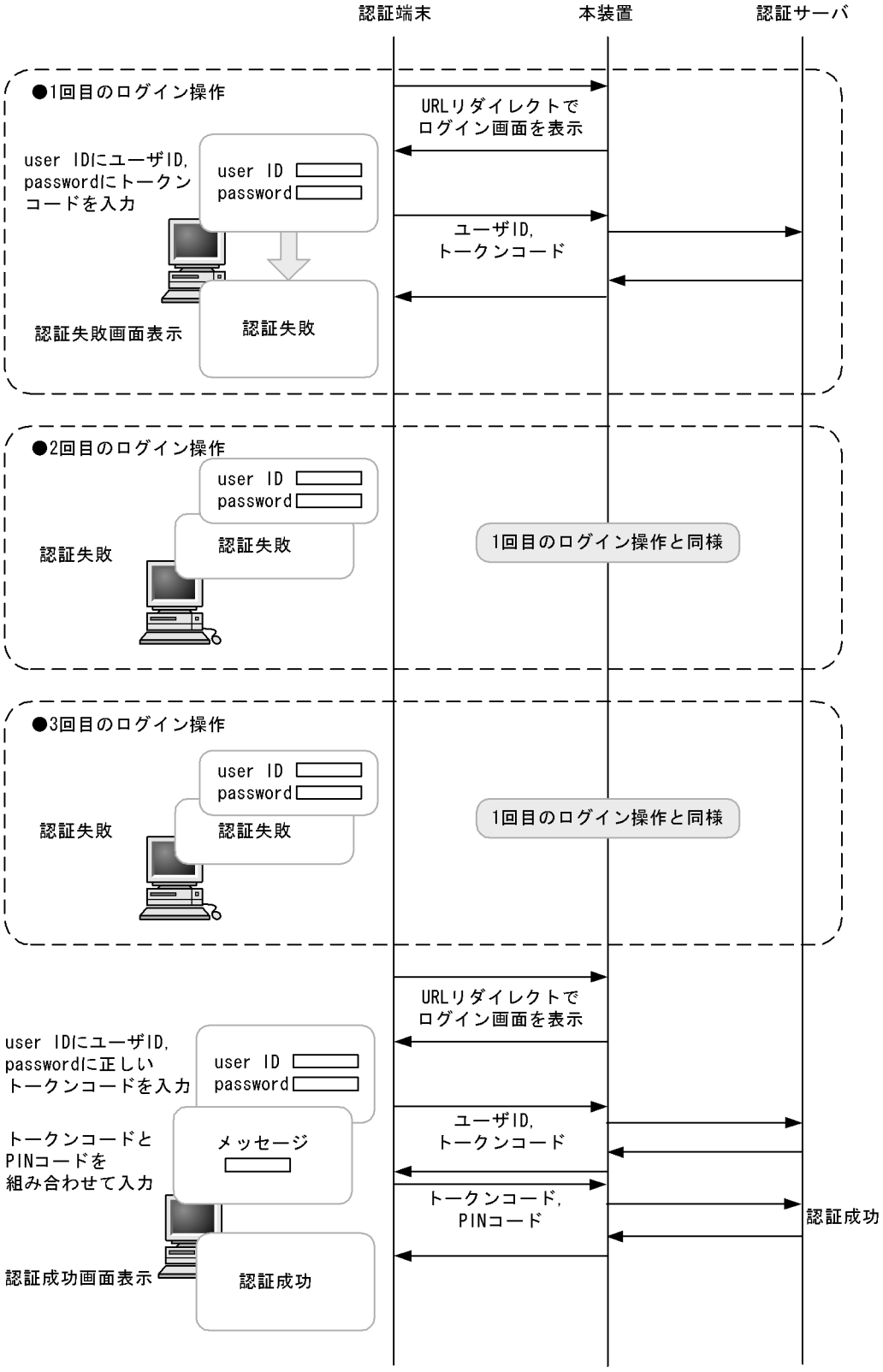
図 8-14　New PIN モードでの動作概要



（2） Next Token モード

ログイン操作時に 3 回連続で不正なトークンコードを入力した場合，次に正しいトークンコードで認証成功したあと，さらに新しいトークンコードの入力を要求するモードです。Next Token モードでの動作概要を次の図に示します。

図 8-15 Next Token モードでの動作概要



8.3.4 強制認証

Web 認証の強制認証については，「5.3 レイヤ 2 認証共通の機能」を参照してください。

8.3.5 認証ネットワークからのログアウト

認証ネットワークにログインした端末をログアウトする方法を次の表に示します。

表 8-1 認証モードごとのログアウト方法

ログアウト方法	固定 VLAN モード	ダイナミック VLAN モード	レガシーモード
Web 画面によるログアウト	○	○	○
最大接続時間超過時のログアウト	○	○	○
認証済み端末の接続監視機能によるログアウト	○	－	－
認証済み端末の MAC アドレステーブルエージングによるログアウト	－	○	○
運用コマンドによるログアウト	○	○	○
認証済み端末からの特殊パケット受信によるログアウト	○	－	－
認証端末接続ポートのリンクダウンによるログアウト	○	－	－
VLAN 設定変更によるログアウト	○	○	○
認証方式の切り替えによるログアウト	○	○	○
認証モードの切り替えによるログアウト	○	○	○
Web 認証の停止によるログアウト	○	○	○
動的に登録された VLAN の削除によるログアウト	－	○	－

（凡例） ○：サポート －：該当なし

ダイナミック VLAN モードおよびレガシーモードの場合，上記の方法でログアウトしたあと，端末の IP アドレスを認証前の IP アドレスに変更してください。また，DHCP サーバを使用している場合は，端末から IP アドレスの再配布を指示してください。

- DHCP サーバを使用している場合，端末の IP アドレスをいったん削除してから，DHCP サーバへ IP アドレスの配布を指示してください。（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。）
- IP アドレスを手動で設定している場合，手動で端末の IP アドレスを認証前の IP アドレスに変更してください。

(1) Web 画面によるログアウト

認証済み端末からログアウト用 URL にアクセスして，端末にログアウト画面を表示させます。画面上のログアウト操作によって Web 認証は認証解除を行います。認証が解除されると，ログアウト完了画面を表示します。

(2) 最大接続時間超過時のログアウト

コンフィグレーションコマンド web-authentication max-timer で設定された最大接続時間を超えた場合に，強制的に Web 認証の認証状態を解除して，端末から本装置外への通信を停止します。この際に設定された最大接続時間が経過してから 1 分以内で認証解除が行われます。この場合には，端末にログアウト完了画面を表示しません。

最大接続時間を超えても使用したい場合は，端末から再度，認証ネットワークへのログイン操作を行ってください。ユーザ ID，パスワードおよび MAC アドレスの組み合わせで認証済みであることが確認された場合に限り，接続時間を延長できます（さらに最大接続時間分だけ延長します）。

なお，コンフィグレーションコマンド web-authentication max-timer で最大接続時間を短縮したり，延長したりした場合，現在認証中のユーザには適用されず，次回ログイン時から設定が有効となります。

(3) 認証済み端末の接続監視機能によるログアウト

認証済み端末に対し，コンフィグレーションコマンド web-authentication logout polling interval で指定された時間間隔で ARP パケットを用い ARP 返答パケットを受信することによって端末の接続監視を行います。コンフィグレーションコマンド web-authentication logout polling retry-interval と web-authentication logout polling count で設定された時間を超えても ARP 返答パケットが受信できない場合，タイムアウトしていると判断し，強制的に Web 認証の認証状態を解除します。この場合には，端末にログアウト完了画面を表示しません。

なお，この機能はコンフィグレーションコマンド no web-authentication logout polling enable で無効にできます。

注意

接続監視機能の設定値としてデフォルトを使用した場合，認証されている数が多いと，接続タイムアウトと判定してから認証が解除されるまで 1 分程度掛かります。
なお，本装置の CPU 負荷が高い場合は，認証解除までさらに時間が掛かることがあります。

(4) 認証済み端末の MAC アドレステーブルエージングによるログアウト

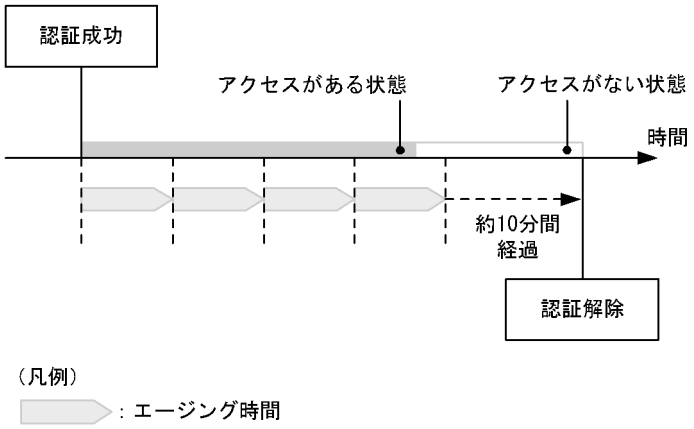
認証済み端末に対し，MAC アドレステーブルを周期的に監視し，端末からのアクセスがあるかをチェックしています。該当する端末からのアクセスがない状態が続いた場合に，強制的に Web 認証の認証状態を解除します。この場合には，端末にログアウト完了画面を表示しません。

ただし，回線の瞬断などの影響で認証が解除されてしまうことを防ぐために，MAC アドレステーブルのエージング時間経過後約 10 分間，該当する MAC アドレスを持つ端末からのアクセスがない状態が続いた場合に，認証状態を解除します。

MAC アドレステーブルのエージング時間と，MAC アドレステーブルエージングによるログアウトの関係を次の図に示します。

なお，MAC アドレステーブルのエージング時間はデフォルト値を使用するか，またはデフォルト値より大きな値を設定してください。

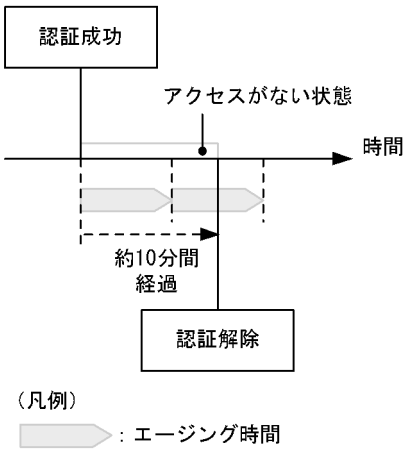
図 8-16　認証済み端末の MAC アドレステーブルエージングによるログアウト



また，認証成功直後約 10 分間に端末からのアクセスがないと，エージング時間の値に関係なく，強制的に認証を解除します。

認証成功直後からアクセスがない場合のログアウトを次の図に示します。

図 8-17　認証成功直後からアクセスがない場合のログアウト



なお，この機能はコンフィグレーションコマンド no web-authentication auto-logout で無効にできます（アクセスがない状態が続いた場合でも強制的にログアウトしない設定が可能）。

さらに，レガシーモードでは，認証後に切り替わった VLAN に端末からの通信がまったくないと，MAC アドレス学習が行われません。この場合，認証済みであっても MAC アドレステーブルに MAC アドレスが登録されていないので，強制的にログアウトします。したがって，認証後は必ず通信を行ってください。

(5) 運用コマンドによるログアウト

運用コマンド clear web-authentication auth-state でユーザ単位に，強制的にログアウトができます。なお，同一ユーザ ID で複数ログインを行っている場合，同じユーザ ID を持つ認証をすべてログアウトします。この場合には，端末にログアウト完了画面を表示しません。

(6) 認証済み端末からの特殊パケット受信によるログアウト

認証済み端末から送信された特殊パケットを受信した場合，該当する端末の認証を解除します。この場合には，端末にログアウト完了画面を表示しません。特殊パケットの条件を次に示します。

- 認証済み端末から Web 認証専用 IP アドレスで送出された ping パケット
- コンフィグレーションコマンド web-authentication logout ping tos-windows で設定された TOS 値を持っているパケット
- コンフィグレーションコマンド web-authentication logout ping ttl で設定された TTL 値を持っているパケット

(7) 認証端末接続ポートのリンクダウンによるログアウト

認証済み端末が接続しているポートのリンクダウンを検出した場合，該当するポートに接続された端末の認証を解除します。この場合には，端末にログアウト完了画面を表示しません。

(8) VLAN 設定変更によるログアウト

コンフィグレーションコマンドで認証端末が含まれる VLAN の設定を変更した場合，変更された VLAN に含まれる端末の認証を解除します。この場合には，端末にログアウト完了画面を表示しません。

［コンフィグレーションの変更内容］

- VLAN を削除した場合
- VLAN を停止（suspend）した場合

(9) 認証方式の切り替えによるログアウト

認証方式が RADIUS 認証方式からローカル認証方式に切り替わった場合，またはローカル認証方式から RADIUS 認証方式に切り替わった場合，すべての端末の認証を解除します。この場合には，端末にログアウト完了画面を表示しません。

(10) 認証モードの切り替えによるログアウト

copy コマンドでコンフィグレーションを変更して，認証モードが切り替わる設定をした場合，すべての端末の認証を解除します。この場合には，端末にログアウト完了画面を表示しません。

(11) Web 認証の停止によるログアウト

コンフィグレーションコマンドで Web 認証の定義が削除されて Web 認証が停止した場合，すべての端末の認証を解除します。この場合には，端末にログアウト完了画面を表示しません。

(12) 動的に登録された VLAN の削除によるログアウト

動的に VLAN が作成された認証ポートにコンフィグレーションコマンド switchport mac vlan が設定された場合，該当ポートに動的に作成された VLAN ID は削除されて，VLAN に所属していた端末の認証を解除します。

8.3.6 認証数制限

装置単位およびポート単位に認証数の制限が設定できます。詳細は，「5.3 レイヤ 2 認証共通の機能」を参照してください。

8.3.7 認証済み端末のポート間移動

認証済み端末がポート間移動した場合については，「5.3 レイヤ 2 認証共通の機能」を参照してください。

8.3.8 アカウント機能

認証結果は次のアカウント機能によって記録されます。

(1) アカウントログ

認証結果は本装置の Web 認証のアカウントログに記録されます。記録されたアカウントログは運用コマンド show web-authentication logging で表示できます。出力される認証結果を次の表に示します。

表 8-2 出力される認証結果

事象	時刻	ユーザ ID	IP アドレス	MAC アドレス	VLAN ID	ポート番号	メッセージ
ログイン成功	○	○	△※1	○	△※1	△	認証成功メッセージ
ログアウト	○	○	△	○※2	△	△	認証解除メッセージ
ログイン失敗	○	○	○※2	○※2	○※2	△※2	失敗要因メッセージ
強制ログアウト	○	○	△※2	○※2	○※2	△※2	強制解除メッセージ

(凡例)
○：固定 VLAN モード，ダイナミック VLAN モード，およびレガシーモードで出力される
△：固定 VLAN モードとダイナミック VLAN モードで出力される
注※1 ダイナミック VLAN モードのログイン成功時に表示される IP アドレスには，認証前の IP アドレスが表示されます。また，VLAN ID には認証後の VLAN ID が表示されます。
注※2 メッセージによっては IP アドレスなどの情報が出力されない場合があります。

本装置の Web 認証のアカウントログは，最大 2100 行まで記録できます。2100 行を超えた場合，古い順に記録が削除され，最新のアカウント情報が追加記録されていきます。

(2) RADIUS サーバのアカウント機能への記録

コンフィグレーションコマンド aaa accounting web-authentication default start-stop group radius を設定すると，RADIUS サーバのアカウント機能を使用できます。アカウント機能には次の情報が記録されます。記録される情報を次に示します。

- ログイン情報　　：ログイン成功時に次の情報が記録されます。
  サーバに記録された時刻，ユーザ ID，MAC アドレス
- ログアウト情報　：ログアウト時に次の情報が記録されます。
  サーバに記録された時刻，ユーザ ID，MAC アドレス，ログインからログアウトまでの経過時間
- 強制ログアウト時：ログアウト時に次の情報が記録されます。
  サーバに記録された時刻，ユーザ ID，MAC アドレス，ログインからログアウトまでの経過時間

(3) RADIUS サーバへのログイン情報記録（RADIUS サーバの機能）

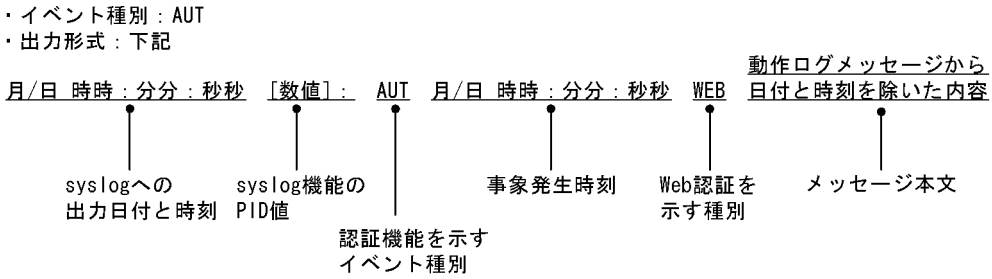
RADIUS 認証方式の場合は，RADIUS サーバが持っている機能によって，ログイン成功／失敗が記録されます。ただし，使用する RADIUS サーバによって記録される情報が異なる場合がありますので，詳細は RADIUS サーバの説明書を参照してください。

(4) syslog サーバへの動作ログ記録

Web 認証の動作ログを syslog サーバに出力できます。また，動作ログは Web 認証のアカウントログを含

みます。syslog サーバへの出力形式を次の図に示します。

図 8-18　syslog サーバへの出力形式



また，コンフィグレーションコマンド web-authentication logging enable および logging event-kind aut によって，出力を開始および停止できます。

8.4 認証手順

Web 認証を用いたユーザ認証は次の手順で行います。Web ブラウザ Internet Explorer Version6.0 を用いて説明します。

(1) Web 認証のログイン画面表示

固定 VLAN モードまたはダイナミック VLAN モードで URL リダイレクト機能を使用する場合は，URL リダイレクト機能によって Web 認証のログイン画面が表示されます。また，Web 認証専用 IP アドレスの URL にアクセスしても Web 認証のログイン画面が表示されます。ログイン画面が表示されたら，ユーザ ID とパスワードを入力します。

［固定 VLAN モードまたはダイナミック VLAN モードのログイン URL 指定］

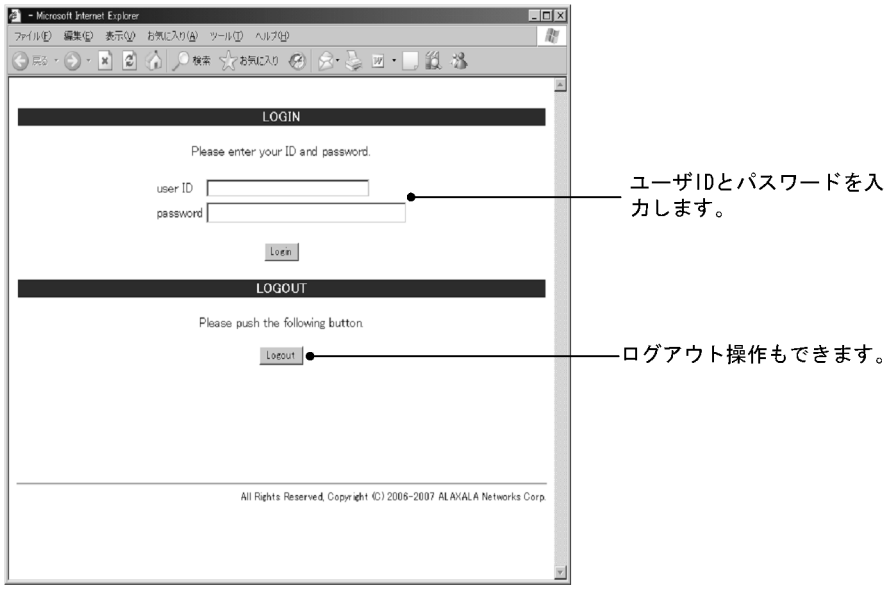
- URL リダイレクト機能無効時の URL 指定：http://Web 認証専用 IP アドレス /login.html
- Web 認証専用 IP アドレスの URL 指定：http://Web 認証専用 IP アドレス /login.html

レガシーモードでは，Web 認証のログイン URL にアクセスすると，Web 認証のログイン画面を表示しますので，ログイン画面からユーザ ID とパスワードを入力します。

［レガシーモードのログイン URL 指定］

- ログイン URL：http:// 認証前 VLAN のインタフェース IP アドレス /login.html

図 8-19 ログイン画面



(2) ログイン画面に入力されたユーザ ID，パスワードの認証

入力されたユーザ ID とパスワードを基に，ローカル認証方式の場合は内蔵 Web 認証 DB に登録されているユーザ情報と一致しているかチェックします。また，RADIUS 認証方式の場合は RADIUS サーバに問い合わせを行い，認証可否のチェックをします。

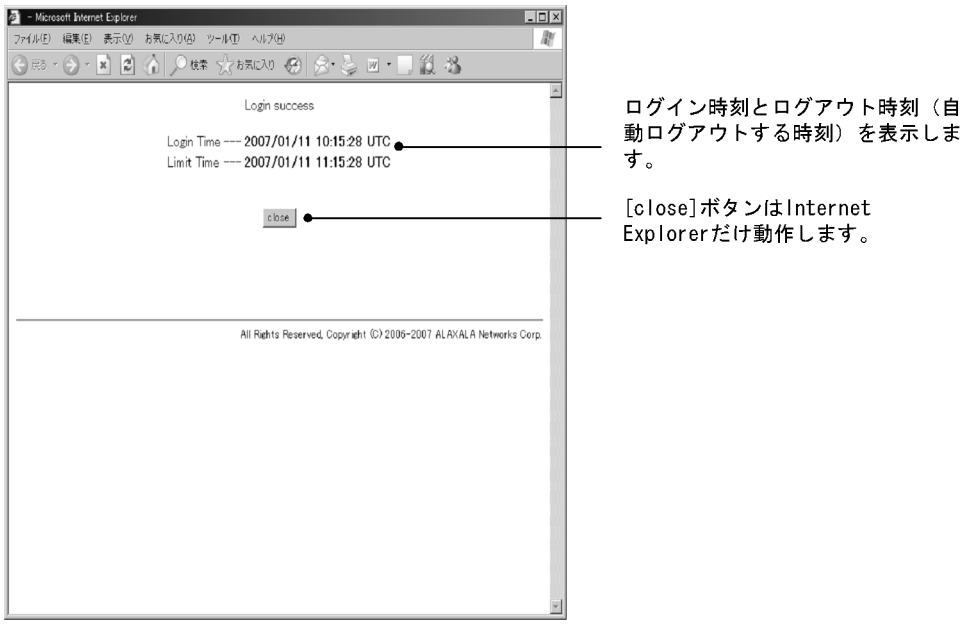
(3) 認証成功結果を表示

内蔵 Web 認証 DB または RADIUS サーバに登録されているユーザ情報と一致した場合，ログイン成功画

面を表示し，認証ネットワークへ通信できます。

また，コンフィグレーションコマンド web-authentication jump-url で認証成功後にアクセスする URL が指定されている場合は，端末にログイン成功画面が表示されたあとに指定された URL へのアクセスが行われます。

図 8-20　ログイン成功画面

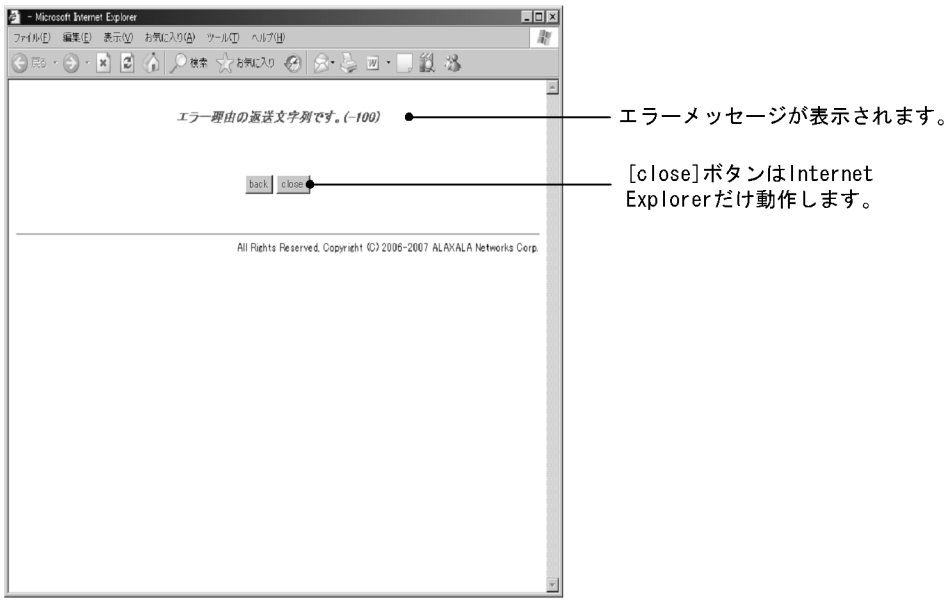


(4) 認証失敗時の画面表示

認証が失敗となった場合は，認証エラー画面を表示します。

認証エラー画面に表示されるエラーの発生理由を，「8.6　認証エラーメッセージ」に示します。

図 8-21　ログイン失敗画面



(5) Web 認証からのログアウト画面表示

認証済み端末から Web 認証のログアウト URL にアクセスして，端末にログアウト画面を表示させます。または，ログイン URL にアクセスして，端末にログイン画面を表示させます。

固定 VLAN モードまたはダイナミック VLAN モードの場合，Web 認証専用 IP アドレスの URL にアクセスします。

［固定 VLAN モードまたはダイナミック VLAN モードのログアウト URL 指定］

- Web 認証専用 IP アドレスのログアウト URL：http://Web 認証専用 IP アドレス /logout.html
- Web 認証専用 IP アドレスのログイン URL：http://Web 認証専用 IP アドレス /login.html

レガシーモードの場合，Web 認証のログアウト URL にアクセスします。

［レガシーモードのログアウト URL 指定］

- ログアウト URL：http:// 認証後 VLAN のインタフェース IP アドレス /logout.html

表示した画面上の［Logout］ボタンを押すと，Web 認証は認証解除を行います。

認証が解除されると，ログアウト完了画面を表示します。

図 8-22　ログアウト画面

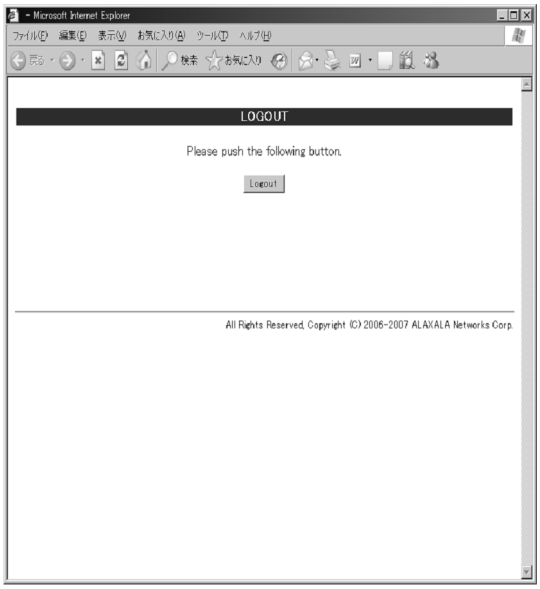
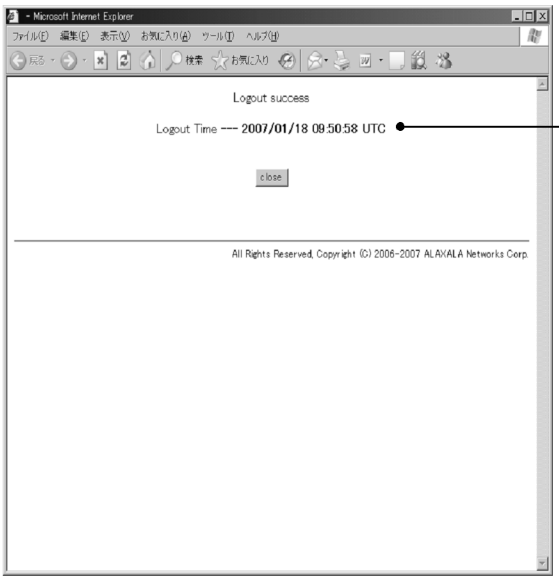


図 8-23 ログアウト完了画面

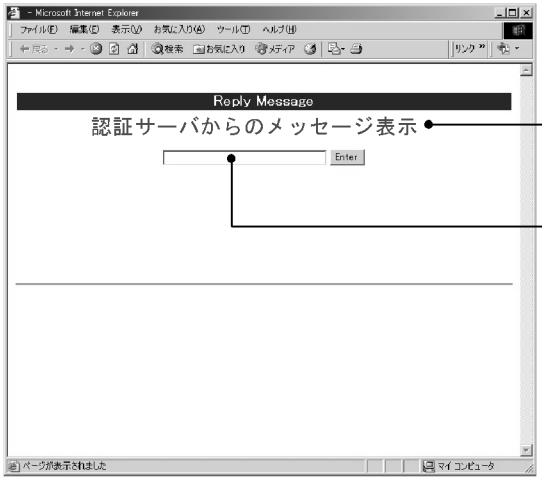


ログアウト時刻（ログアウト動作が完了した時刻）を表示します。

(6) ワンタイムパスワード認証の Reply-Message 表示画面表示【OP-OTP】

ワンタイムパスワード認証で表示する Reply-Message 表示画面を次に示します。Reply-Message 表示画面に表示されたメッセージに従って，新しい PIN コード，またはトークンコードを入力します。

図 8-24 Reply-Message 表示画面



認証サーバから送られてきたメッセージを表示します。

メッセージに従って，PINコードまたはトークンコードを入力します。

8.5 内蔵 Web 認証 DB および RADIUS サーバの準備

8.5.1 内蔵 Web 認証 DB の準備

Web 認証のローカル認証方式を使用するに当たっては，事前に内蔵 Web 認証 DB を作成する必要があります。また，本装置の内蔵 Web 認証 DB はバックアップおよび復元できます。

(1) 内蔵 Web 認証 DB の作成

運用コマンド set web-authentication user で，ユーザ ID，パスワード，VLAN ID などのユーザ情報を内蔵 Web 認証 DB に登録します。また，登録したユーザ ID ごとのパスワード変更および削除もできます。

登録・変更された内容は，運用コマンド commit web-authentication が実行された時点で，内蔵 Web 認証 DB に反映されます。

なお，運用コマンドで内蔵 Web 認証 DB への追加および変更を行った場合，現在認証中のユーザには適用されず，次回ログイン時から有効となります。

(2) 内蔵 Web 認証 DB のバックアップ

運用コマンド store web-authentication で，ローカル認証用に作成した内蔵 Web 認証 DB のバックアップを取ることができます。

(3) 内蔵 Web 認証 DB の復元

運用コマンド load web-authentication で，ローカル認証用に作成したバックアップファイルから，内蔵 Web 認証 DB の復元ができます。ただし，復元を実行すると，直前に運用コマンド set web-authentication user などで登録・更新していた内容は廃棄されて，復元された内容に置き換わりますので，注意が必要です。

8.5.2 RADIUS サーバの準備

Web 認証の RADIUS 認証方式を使用するに当たっては，事前に RADIUS サーバの設定が必要です。

また，本装置の Web 認証機能が使用する RADIUS の属性を示します。

(1) RADIUS サーバの設定

ユーザごとにユーザ ID，パスワード，VLAN ID などのユーザ情報を RADIUS サーバに設定します。なお，RADIUS サーバの詳細な設定方法については，使用する RADIUS サーバの説明書を参照してください。

ダイナミック VLAN モードで認証成功後に切り替える認証後 VLAN を次のように設定します。

1. Tunnel-Type に Virtual LANs（VLAN）を設定（値 13）します。
2. Tunnel-Medium-Type に 6 を設定します。
3. Tunnel-Private-Group-ID に VLAN ID を次の形式で設定します。

- 数字文字で設定
  例：VLAN ID が 2048 の場合，文字列で 2048 を設定
- 文字列 ” VLAN ” に続いて VLAN ID を数字文字で設定
  例：VLAN ID が 2048 の場合，VLAN2048 を設定

- コンフィグレーションコマンド name で設定した VLAN 名称を設定

なお，Tunnel-Type，Tunnel-Medium-Type，および Tunnel-Private-Group-ID の三つの属性がすべて設定されていない状態でダイナミック VLAN モードで使用した場合，認証後 VLAN としてネイティブ VLAN を適用します。

ユーザ ID とパスワードには文字数 1 ～ 32 文字で，次の文字が使用できます。

- ユーザ ID：ASCII 文字コードの 0x21 ～ 0x7E
- パスワード：ASCII 文字コードの 0x21 ～ 0x7E

また，認証方式として PAP を設定します。

(2) Web 認証が使用する RADIUS 属性

Web 認証が使用する RADIUS の属性を次の表に示します。

表 8-3 認証で使用する属性名（その 1 Access-Request）

属性名	Type 値	説明
User-Name	1	ユーザ名を指定します。
User-Password	2	ユーザパスワードを指定します。
NAS-IP-Address	4	ループバックインタフェースの IP アドレス指定時はループバックインタフェースの IP アドレスを格納し，指定されていなければ RADIUS サーバと通信するインタフェースの IP アドレスを格納します。
Service-Type	6	Framed(2) を設定します。
State	24	該当する認証に対して，直前に RADIUS サーバから Access-Challenge で送られてきた State 値を設定します。 なお，State 値がない場合は設定しません。
Calling-Station-Id	31	認証端末の MAC アドレス（小文字 ASCII，“ - ” 区切り）を指定します。 例：00-12-e2-12-34-56
NAS-Identifier	32	固定 VLAN モード時に認証端末を収容している VLAN ID を数字文字列で指定します。 例：VLAN ID 100 の場合 100 ダイナミック VLAN モードおよびレガシーモードでは，コンフィグレーションコマンド hostname で指定された装置名を指定します。
NAS-Port-Type	61	Virtual(5) を設定します。
NAS-IPv6-Address	95	ループバックインタフェースの IPv6 アドレス指定時はループバックインタフェースの IPv6 アドレスを格納し，指定されていなければ RADIUS サーバと通信するインタフェースの IPv6 アドレスを格納します。ただし，IPv6 リンクローカルアドレスで通信する場合は，ループバックインタフェースの IPv6 アドレス設定の有無にかかわらず，送信インタフェースの IPv6 リンクローカルアドレスを格納します。

表 8-4 認証で使用する属性名（その 2 Access-Accept）

属性名	Type 値	説明
Service-Type	6	Framed(2) が返却される：Web 認証ではチェックしません。
Reply-Message	18	（未使用）

属性名	Type 値	説明
Tunnel-Type	64	ダイナミック VLAN モードおよびレガシーモード時に使用します。 VLAN を示す 13 であるかをチェックします。 固定 VLAN モード時は使用しません。
Tunnel-Medium-Type	65	ダイナミック VLAN モードおよびレガシーモード時に使用します。 IEEE802.1X と同様の値 6 の Tunnel-Medium-Type であるかをチェックします。 固定 VLAN モード時は使用しません。
Tunnel-Private-Group-Id	81	ダイナミック VLAN モードおよびレガシーモード時に使用します。 VLAN を表す数字文字列または " VLANxx " xx は VLAN ID を表します。 ただし，先頭の 1 オクテットの内容が 0x00 ～ 0x1f の場合は，Tag を表しているので，この場合は 2 オクテット目からの値が VLAN を表します。先頭の 1 オクテットの内容が 0x20 以上の場合は，先頭から VLAN を表します。 また，ダイナミック VLAN モードでは，コンフィグレーションコマンド name で設定された VLAN 名称が指定された場合，VLAN 名称に対応する VLAN ID を使用します。 固定 VLAN モード時は使用しません。

表 8-5　ワンタイムパスワード認証で使用する属性名（その 3　Access-Challenge）【OP-OTP】

属性名	Type 値	説明
Reply-Message	18	テキスト文字列 ワンタイムパスワード認証で使用するメッセージを Reply-Message 表示画面に表示します。
State	24	ワンタイムパスワード認証で使用する次の Access-Request の State 値として使用します。

表 8-6　RADIUS Accounting で使用する属性名

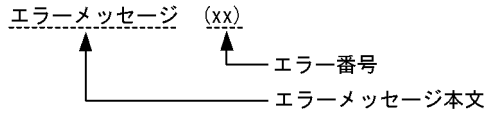
属性名	Type 値	説明
User-Name	1	利用者のユーザ名称を格納します。
NAS-IP-Address	4	NAS の IP アドレスを格納します。 ループバックインタフェースの IP アドレス設定時は，ループバックインタフェースの IP アドレスを格納します。なお，上記以外はサーバと通信するインタフェースの IP アドレスを格納します。
Service-Type	6	Framed(2) を設定します
Calling-Station-Id	31	端末の MAC アドレス（小文字 ASCII, " - " 区切り）を設定します。 例：00-12-e2-12-34-56
NAS-Identifier	32	固定 VLAN モード時に認証端末を収容している VLAN ID を数字文字列で設定します。 例：VLAN ID 100 の場合 100 ダイナミック VLAN モードおよびレガシーモードでは，コンフィグレーションコマンド hostname で指定された装置名を指定します。
Acct-Status-Type	40	ログイン時に Start(1)，ログアウト時に Stop(2) を格納します。
Acct-Delay-Time	41	イベント発生時から送信するまでに必要とした時間（秒）を格納します。
Acct-Session-Id	44	プロセス ID を格納します。（ログイン，ログアウトに関しては同じ値です）
Acct-Authentic	45	ユーザがどのように認証されたかを示す RADIUS，Local のどちらかを格納します。

属性名	Type 値	説明
Acct-Session-Time	46	ログイン後ログアウトするまでの時間（秒）を格納します。
NAS-Port-Type	61	Virtual(5) を設定します。
NAS-IPv6-Address	95	NAS の IPv6 アドレスを格納します。 ループバックインタフェースの IPv6 アドレス設定時は，ループバックインタフェースの IPv6 アドレスを格納します。なお，上記以外はサーバと通信するインタフェースの IPv6 アドレスを格納します。ただし，IPv6 リンクローカルアドレスで通信する場合は，ループバックインタフェースの IPv6 アドレス設定の有無にかかわらず，送信インタフェースの IPv6 リンクローカルアドレスを格納します。

8.6 認証エラーメッセージ

認証エラー画面に表示される認証エラーメッセージ表示の形式を次の図に示します。

図 8-25 認証エラーメッセージ形式



認証エラーの発生理由を次の表に示します。

表 8-7 認証エラーメッセージとエラー発生理由対応表

エラーメッセージ内容	エラー番号	エラー発生理由
User ID or password is wrong. Please enter correct user ID and password.	11	ログインユーザ ID が指定されていません
	12	ログインユーザ ID が 32 文字を超えています
	13	パスワードが指定されていない，または指定された文字数が長過ぎます
	14	ログインユーザ ID が内蔵 Web 認証 DB に登録されていません
	15	パスワードが内蔵 Web 認証 DB に登録されていません
	16	GET メソッドの "QUERY_STRING" が 21 文字未満か，または，256 文字を超えています
	17	POST メソッドの " CONTENT_LENGTH" が 21 未満である，または 340 を超えています
	18	ログインユーザ ID に許可されていない文字が指定されています
	20	パスワードに許可されていない文字が指定されています
	22	ローカル認証方式で，認証済みの端末から再ログインを行った際，パスワードが一致していませんでした
RADIUS: Authentication reject.	31	RADIUS サーバから認証許可以外（アクセス拒否またはアクセスチャレンジ）を受信しました
RADIUS: No authentication response.	32	RADIUS サーバから認証許可を受信できませんでした（受信タイムアウト，または RADIUS サーバの設定がされていない状態です）
You cannot login by this machine.	33	RADIUS に設定されている認証後 VLAN が，Web 認証で定義された VLAN ではありません。 または，VLAN インタフェースに設定されていません
	34	RADIUS 認証方式で，認証済み端末から再ログインを行った際に RADIUS サーバから認証許可以外（アクセス拒否またはアクセスチャレンジ）を受信しました
	35	固定 VLAN モードで，端末が接続されている認証対象ポートがリンクダウンの状態です。 または，ポートが固定 VLAN モードとして設定されていません

エラーメッセージ内容	エラー番号	エラー発生理由
	36	固定 VLAN モードで設定されたポートを収容する VLAN が suspend 状態になっています。 または，VLAN がインタフェースに設定されていません
	41	Web 認証で認証済みの端末から，異なるユーザでのログイン要求がありました。 または，ダイナミック VLAN モードで，異なる VLAN から認証済み端末のログイン要求がありました
	42	内蔵 Web 認証 DB に設定された VLAN ID が，Web 認証で定義された VLAN ではありません。 または，VLAN インタフェースに設定されていません
	44	同一端末で，IEEE802.1X もしくは MAC 認証によって認証済み，またはコンフィグレーションコマンド mac-address で端末の MAC アドレスが MAC VLAN に登録済みのため認証できません
	45	端末が接続されている認証対象ポートがリンクダウンの状態です。 または，ポートが固定 VLAN モードもしくはダイナミック VLAN モードとして設定されていません
	46	認証対象ポートを収容する VLAN が suspend 状態となっています。 または，VLAN がインタフェースに設定されていません
	47	Web 認証のログイン数が最大収容条件を超えたために認証できませんでした
	76	MAC アドレスを MAC アドレステーブルに登録する際，端末が接続されているポートがリンクダウンしています。 または，ポートが固定 VLAN モードもしくはダイナミック VLAN モードとして設定されていません
	77	MAC アドレスを MAC アドレステーブルに登録する際，収容する VLAN が suspend 状態になっています。 または，VLAN がインタフェースに設定されていません
Sorry, you cannot login just now. Please try again after a while.	37	RADIUS 認証途中の認証要求が 256 件を超えています。 再度，ログイン操作を行ってください
	43	Web 認証，MAC 認証，または IEEE802.1X 認証のログイン数が装置最大収容条件を超えたために認証できませんでした
	48	認証対象ポートの認証制限数を超えたために認証できませんでした
	51	ログイン端末の IP アドレスから MAC アドレスを解決できませんでした
	52	Web サーバが，Web 認証デーモンと接続できませんでした
	53	Web 認証の内部エラー (Web サーバが，Web 認証デーモンにログイン要求を渡せませんでした)
	54	Web 認証の内部エラー (Web サーバが，Web 認証デーモンから応答を受け付けられませんでした)
The system error occurred. Please contact the system administrator.	61	Web 認証の内部エラー (POST メソッドの " CONTENT_LENGTH" が取得できませんでした)

エラーメッセージ内容	エラー番号	エラー発生理由
	62	Web 認証の内部エラー (POST/GET で受け取ったパラメータに ” & ” が 2 個以上含まれていました)
	63	Web 認証の内部エラー (Web サーバで端末の IP アドレスが取得できませんでした)
	64	RADIUS および Accounting へのアクセスができませんでした (認証失敗となります)
A fatal error occurred. Please inform the system administrator.	65	Web 認証の内部エラー (同時に 256 件を超えた RADIUS への認証要求が起きました)
	72	MAC VLAN に認証した MAC アドレスを登録できませんでした
	73	MAC VLAN から認証解除する MAC アドレスを削除できませんでした
	74	MAC アドレスを MAC アドレステーブルに登録する際にエラーが発生しました
	75	MAC アドレステーブルから MAC アドレスを削除する際にエラーが発生しました
Sorry, you cannot logout just now. Please try again after a while.	81	ログアウト要求された端末の IP アドレスから MAC アドレスを解決できませんでした
The client PC is not authenticated.	82	ログインされていない端末からのログアウト要求です

エラー番号ごとの対処方法

- 1x ～ 2x：正しいユーザ ID とパスワードで再度ログイン操作を行ってください。
- 3x：RADIUS の設定を見直してください。
- 4x：Web 認証のコンフィグレーション，および内蔵 Web 認証 DB の設定を見直してください。
- 5x：再度ログイン操作を行ってください。再び本メッセージが表示される場合は，運用コマンド restart web-authentication で Web 認証を再起動してください。
- 6x ～ 7x：運用コマンド restart web-authentication で Web 認証を再起動してください。
- 8x：再度ログアウト操作を行ってください。

8.7 Web 認証画面入れ替え機能

Web 認証で使用するログイン画面やログアウト画面など，Web ブラウザに表示する画面情報（以降，Web 認証画面と呼びます）は，運用コマンドで入れ替えることができます。その運用コマンドで指定したディレクトリ配下に，次に示す画面のファイルがあった場合，該当する Web 認証画面と置き換えます。また，次に示すファイル以外に gif ファイルなどの画像ファイルも同時に登録できます。ただし，登録時には各ファイルのサイズチェックだけを行い，ファイルの内容はチェックしませんので，必ず動作確認を行ってから HTML ファイルや画像ファイルを登録してください。

入れ替えることができる画面を次に示します。

［入れ替え可能な画面］
- ログイン画面
- ログアウト画面
- ログイン成功画面
- ログイン失敗画面
- ログアウト完了画面
- ログアウト失敗画面
- Reply-Message 表示画面

なお，登録した Web 認証画面は運用コマンドで削除できます。削除したあとは，デフォルトの Web 認証画面に戻ります。

また，「表 8-7　認証エラーメッセージとエラー発生理由対応表」に示す認証エラーメッセージも入れ替えることができます。

さらに，Web ブラウザのお気に入りに表示するアイコン（favicon.ico）も入れ替えることができます。

各ファイルの詳細は，「9.3　Web 認証画面作成手引き」を参照してください。

なお，Web 認証画面の登録中に次に示すような中断が起きた場合，登録した画面が表示されずにデフォルト画面が表示されます。このとき，運用コマンド show web-authentication html-files で Web 認証画面の登録情報を表示すると，登録が成功したかのように表示されることがあります。

- Web 認証画面登録中に［Ctrl］＋［C］キーを押して，意図的に処理を中断させた場合
- telnet 経由でコンソールにログインし，Web 認証画面登録中に telnet が何らかの要因で切断された場合

Web 認証画面の登録中に中断が起きた場合は，再度 Web 認証画面を登録してください。

8.8 Web 認証使用時の注意事項

(1) 他機能との共存

他機能との共存については，「5.2 レイヤ 2 認証と他機能との共存について」を参照してください。

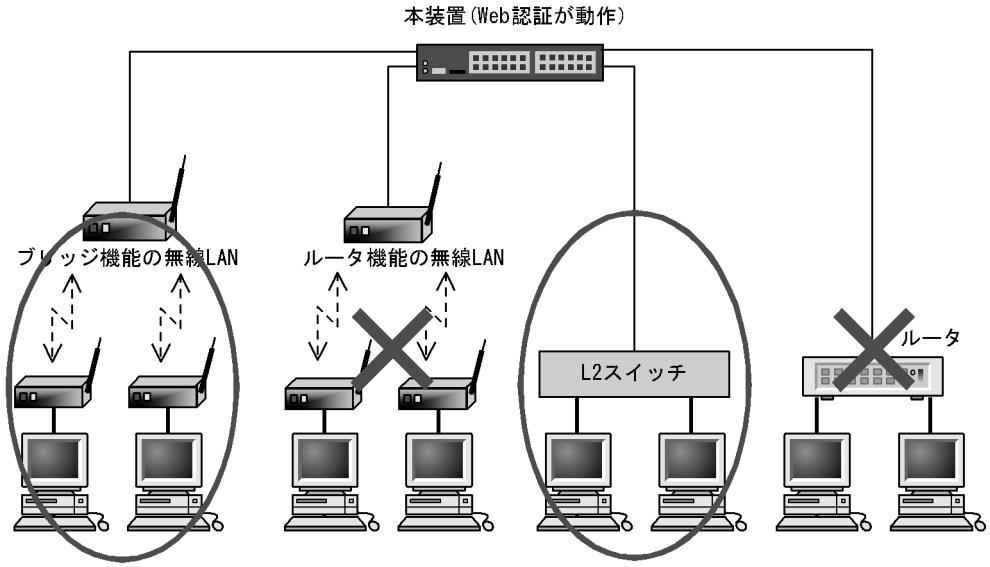
(2) 本装置と認証対象の端末間に接続する装置について

本装置の配下にはプロキシサーバやルータを接続しないでください。

本装置と認証端末との間の経路上に，クライアント端末の MAC アドレスを書き換えるもの（プロキシサーバやルータなど）が存在した場合，Web 認証が書き換えられた MAC アドレスを認証対処端末と認識してしまうために端末ごとの認証ができません。

また，本装置の配下にポート間遮断機能の無い HUB や無線 LAN を接続し，それに複数の PC が接続されている場合，認証済みでなくても PC 同士で通信ができてしまいますので注意が必要です。

図 8-26 本装置と端末間の接続

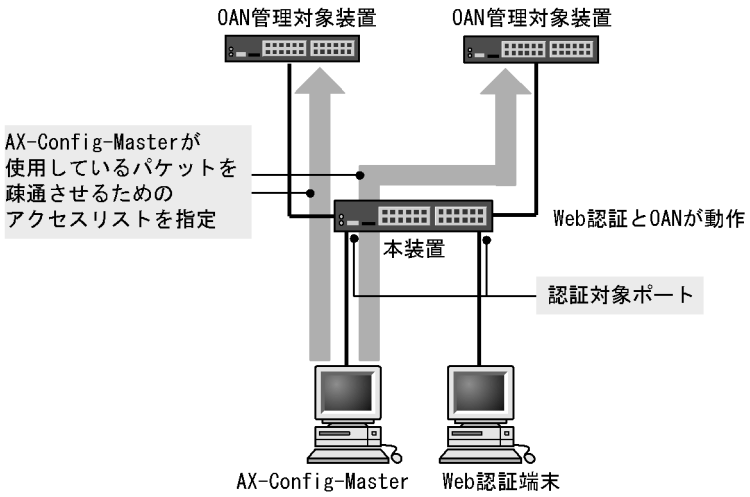


(3) OAN との共存について

Web 認証は OAN と共存できますが，固定 VLAN モードおよびダイナミック VLAN モードが有効な場合，次に示す条件があります。

- 本装置の認証対象ポートに AX-Config-Master を接続し，Web 認証を行わずに本装置で使用したい場合は，コンフィグレーションコマンド web-authentication web-port で OAN が使用する https ポート（832，9698）を指定する必要があります。
- 認証対象ポートに AX-Config-Master を接続し，Web 認証を行わずに本装置の外部に接続された装置を管理する場合，次の図に示すようにアクセスリストで OAN が使用する IP パケットを通信させる設定が必要です。

図 8-27 OAN との共存



(4) VLAN 機能が再起動した場合の動作

運用コマンド restart vlan で VLAN 機能が再起動した場合，Web 認証は認証を解除しないで，認証された順に再登録をします。ただし，認証数が多い場合，登録に時間が掛かるため，登録が完了するまでの間通信ができなくなりますが，登録が完了した時点で通信ができます。

(5) Web 認証プログラムが再起動した場合

Web 認証デーモンが再起動した場合，認証中のユーザすべての認証が解除されます。この場合，再起動後に端末から手動で再度認証を行ってください。

(6) DHCP サーバの IP アドレスリース時間設定について

認証対象端末に認証前 IP アドレスを DHCP サーバから配布する場合，DHCP サーバの IP アドレスリース時間をできるだけ短く設定してください。

なお，内蔵 DHCP サーバに関しては，10 秒から指定できますが，小さい値を設定し，しかも，認証ユーザ数が多い場合には装置に負荷が掛かりますので，必要に応じてリース時間の設定を変更してください。

(7) レガシーモードでの再認証時の認証後 VLAN について

レガシーモードで，認証済みの端末から認証済みのユーザ ID でログイン操作（再認証操作）を行って認証成功となった際，RADIUS サーバから送られてくる VLAN ID または内蔵 Web 認証 DB に設定された VLAN ID に変更があっても，すでに収容されている VLAN から変更はありません。

ローカル認証方式の場合も RADIUS 認証方式の場合も同様に，最初に認証成功となった時点で収容した認証後 VLAN からの変更は行いません。

9 Web 認証の設定と運用

Web 認証は，Web ブラウザを用いて認証されたユーザ単位に VLAN へのアクセス制御を行う機能です。この章では Web 認証のオペレーションについて説明します。

9.1 コンフィグレーション

9.1.1 コンフィグレーションコマンド一覧

Web 認証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 9-1 コンフィグレーションコマンド一覧

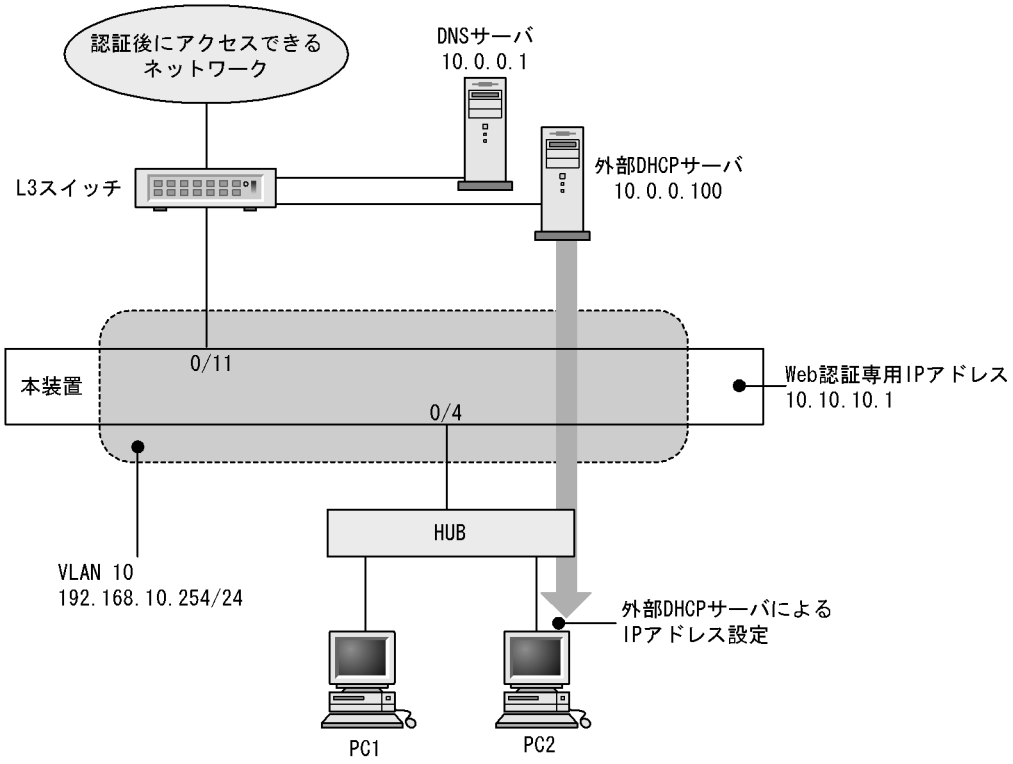
コマンド名	説明
aaa accounting web-authentication default start-stop group radius	アカウンティングサーバの使用設定をします。
aaa authentication web-authentication default group radius	RADIUS サーバの使用設定をします。
web-authentication auto-logout	MAC アドレス学習エージアウトによる強制ログアウト機能を設定します。
web-authentication ip address	固定 VLAN モード時およびダイナミック VLAN モード時の Web 認証専用 IP アドレスを指定します。
web-authentication jump-url	認証成功後，端末からアクセスする URL を指定します。
web-authentication logging enable	認証結果と動作ログの syslog サーバへの出力を開始します
web-authentication logout ping tos-windows	認証済み端末から送出される特殊 ping の TOS 値を指定します。
web-authentication logout ping ttl	認証済み端末から送出される特殊 ping の TTL 値を指定します。
web-authentication logout polling count	監視パケットに対する応答が無かった場合の再送する監視パケットの再送回数を指定します。
web-authentication logout polling enable	認証済み端末の動作を監視する接続監視機能を有効にします。
web-authentication logout polling interval	接続監視機能で使用する監視パケット (ARP) の送出時間を指定します。
web-authentication logout polling retry-interval	監視パケットに対する応答が無い場合に再送する監視パケットの時間間隔を指定します。
web-authentication max-timer	Web 認証の最大接続時間を指定します。
web-authentication max-user	Web 認証でダイナミック VLAN モードおよびレガシーモードの時に認証できる最大認証数を指定します。
web-authentication port	固定 VLAN モードおよびダイナミック VLAN モードの認証対象となるポートを指定します。
web-authentication redirect enable	URL リダイレクト機能を有効にします。
web-authentication redirect-mode	URL リダイレクト時，端末に表示するログイン操作のプロトコル（http または https）を指定します。
web-authentication static-vlan max-user	固定 VLAN モードで認証できるユーザ数を指定します。
web-authentication system-auth-control	Web 認証を有効にします。
web-authentication vlan	レガシーモードで，Web 認証で切り替えを許可する切り替え後の VLAN を指定します。
web-authentication web-port	Web サーバへのアクセスポート番号を追加した場合に指定します。

9.1.2 固定 VLAN モードのコンフィグレーション

(1) ローカル認証方式の基本的な設定

ローカル認証方式を使用する上での基本的な設定を次の図に示します。

図 9-1 固定 VLAN モードのローカル認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1. **(config)# vlan 10**
   (config-vlan)# state active
   (config-vlan)# exit
2. **(config)# interface gigabitethernet 0/4**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# web-authentication port
   (config-if)# exit

   認証を行う端末が接続されているポートに VLAN ID と Web 認証を設定します。

3. **(config)# interface gigabitethernet 0/11**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# exit

認証後にアクセスするネットワークの L3 スイッチを接続するポートを指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

Web 認証で使用する VLAN に IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface vlan 10**
   (config-if)# ip address 192.168.10.254 255.255.255.0
   (config-if)# exit
   Web 認証で使用する VLAN ID 10 に IP アドレスを設定します。

(c) 認証専用 IPv4 アクセスリストの設定

[設定のポイント]

認証前状態の端末から本装置の外部への通信を許可する認証専用 IPv4 アクセスリストを設定します。

[コマンドによる設定]

1. **(config)# ip access-list extended 100**
   (config-ext-nacl)# permit udp any any eq bootps
   (config-ext-nacl)# permit udp any any eq domain
   (config-ext-nacl)# exit
   (config)# interface gigabitethernet 0/4
   (config-if)# authentication ip access-group 100
   (config-if)# authentication arp-relay
   (config-if)# exit
   認証前の端末から DHCP パケットと DNS サーバへのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。さらに，ARP パケットを本装置の外部に転送させるように設定します。

(d) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

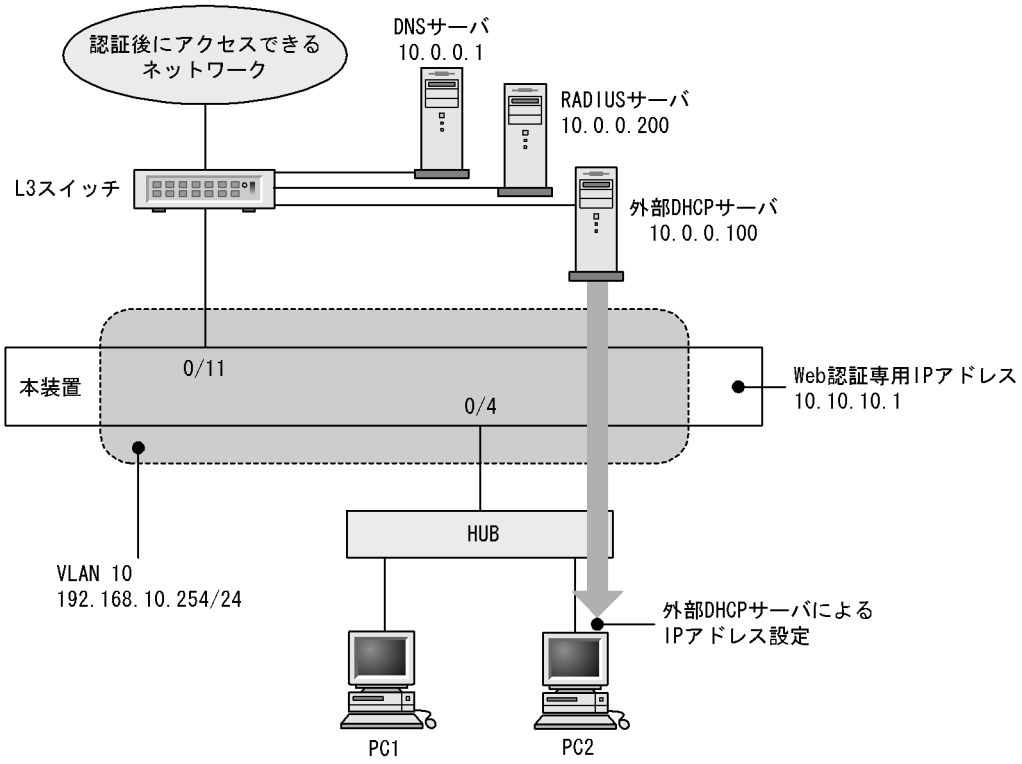
1. **(config)# web-authentication ip address 10.10.10.1**
   Web 認証専用の IP アドレス（IPv4 アドレス）を設定します。

2. **(config)# web-authentication system-auth-control**
   Web 認証を起動します。

(2) RADIUS 認証方式の基本的な設定

RADIUS 認証方式を使用する上での基本的な設定を次の図に示します

図 9-2 固定 VLAN モードの RADIUS 認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1. **(config)# vlan 10**
   (config-vlan)# state active
   (config-vlan)# exit
2. **(config)# interface gigabitethernet 0/4**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# web-authentication port
   (config-if)# exit

   認証を行う端末が接続されているポートに VLAN ID と Web 認証を設定します。

3. **(config)# interface gigabitethernet 0/11**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# exit

   認証後にアクセスするネットワークの L3 スイッチを接続するポートを指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

Web 認証で使用する VLAN に IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface vlan 10**
   (config-if)# ip address 192.168.10.254 255.255.255.0
   (config-if)# exit
   Web 認証で使用する VLAN ID 10 に IP アドレスを設定します。

(c) 認証専用 IPv4 アクセスリストの設定

[設定のポイント]

認証前状態の端末から本装置の外部への通信を許可する認証専用 IPv4 アクセスリストを設定します。

[コマンドによる設定]

1. **(config)# ip access-list extended 100**
   (config-ext-nacl)# permit udp any any eq bootps
   (config-ext-nacl)# permit udp any any eq domain
   (config-ext-nacl)# exit
   (config)# interface gigabitethernet 0/4
   (config-if)# authentication ip access-group 100
   (config-if)# authentication arp-relay
   (config-if)# exit
   認証前の端末から DHCP パケットと DNS サーバへのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。さらに，ARP パケットを本装置の外部に転送させるように設定します。

(d) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

1. **(config)# web-authentication ip address 10.10.10.1**
   Web 認証専用の IP アドレス（IPv4 アドレス）を設定します。

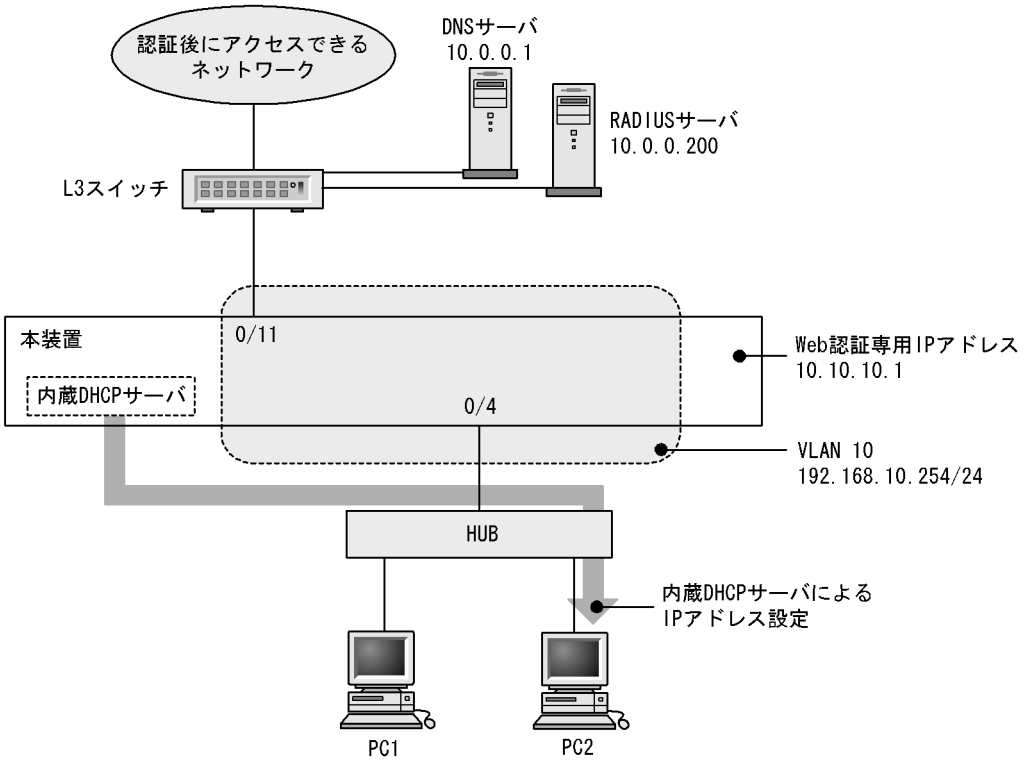
2. **(config)# aaa authentication web-authentication default group radius**
   (config)# radius-server host 10.0.0.200 key "webauth"
   ユーザ認証を RADIUS サーバで行うための IP アドレスと RADIUS 鍵を設定します。

3. **(config)# web-authentication system-auth-control**
   Web 認証を起動します。

(3) RADIUS 認証方式＋内蔵 DHCP サーバ使用時の設定

RADIUS 認証方式と本装置内 DHCP サーバを使用する上での基本的な構成を次の図に示します。

図 9-3 固定 VLAN モードの RADIUS 認証方式＋内蔵 DHCP サーバの基本構成



(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# web-authentication port
   (config-if)# exit
   認証を行う端末が接続されているポートに VLAN ID と Web 認証を設定します。

2. **(config)# interface gigabitethernet 0/11**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# exit
   認証後にアクセスするネットワークの L3 スイッチを接続するポートを指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

Web 認証で使用する VLAN に IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface vlan 10**
   (config-if)# ip address 192.168.10.254 255.255.255.0
   (config-if)# exit
   Web 認証で使用する VLAN ID 10 に IP アドレスを設定します。

(c) 認証専用 IPv4 アクセスリストの設定

[設定のポイント]

認証前状態の端末から本装置の外部への通信を許可する認証専用 IPv4 アクセスリストを設定します。

[コマンドによる設定]

1. **(config)# ip access-list extended 100**
   (config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.10.254 eq bootps
   (config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
   (config-ext-nacl)# permit udp any any eq domain
   (config-ext-nacl)# exit
   (config)# interface gigabitethernet 0/4
   (config-if)# authentication ip access-group 100
   (config-if)# authentication arp-relay
   (config-if)# exit
   認証前の端末から本装置内 DHCP サーバ向けの DHCP パケットと DNS サーバへのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。さらに，ARP パケットを本装置の外部に転送させるよう設定します。

(d) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

1. **(config)# web-authentication ip address 10.10.10.1**
   Web 認証専用の IP アドレス（IPv4 アドレス）を設定します。

2. **(config)# aaa authentication web-authentication default group radius**
   (config)# radius-server host 10.0.0.200 key "webauth"
   ユーザ認証を RADIUS サーバで行うための IP アドレスと RADIUS 鍵を設定します。

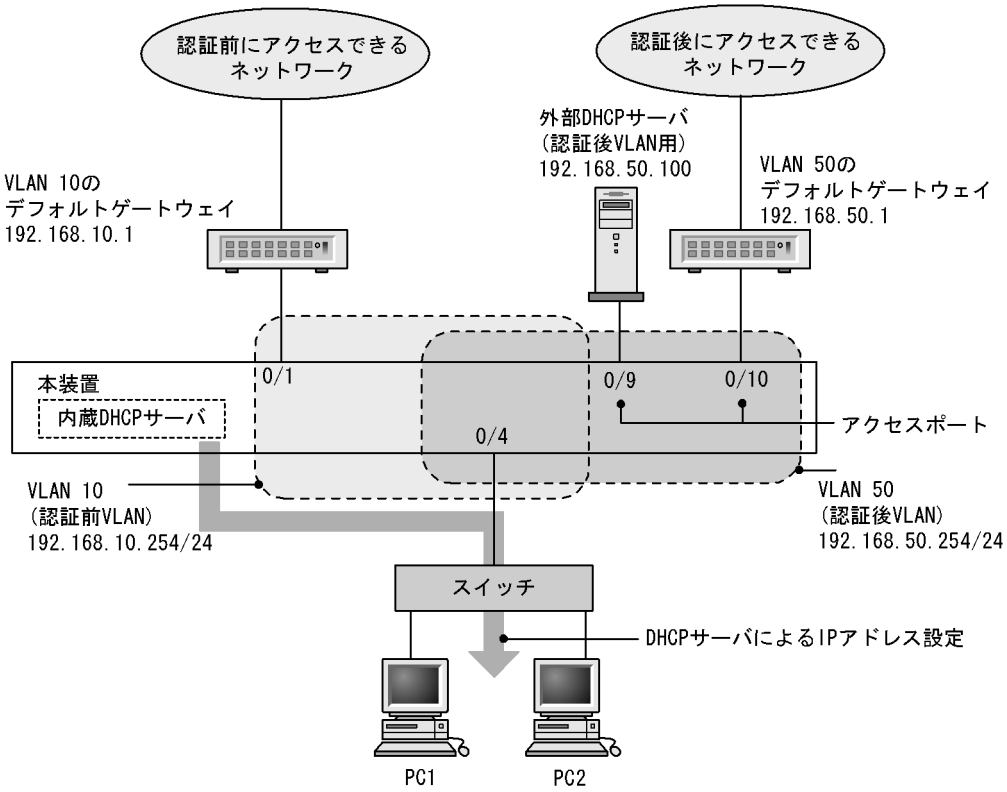
3. **(config)# web-authentication system-auth-control**
   Web 認証を起動します。

9.1.3 ダイナミック VLAN モードのコンフィグレーション

(1) ローカル認証方式の基本的な設定

ローカル認証方式を使用する際の基本的な設定を次の図に示します。なお，端末の IP アドレスは，認証前は本装置内 DHCP サーバから配布し，認証後は外部 DHCP サーバから配布します。

図 9-4 ダイナミック VLAN モードのローカル認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1.
```
(config)# interface gigabitethernet 0/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac native vlan 10
(config-if)# web-authentication port
(config-if)# exit
```
認証を行う端末が接続されているポートに MAC VLAN と Web 認証を設定します。

2.
```
(config)# interface range gigabitethernet 0/9-10
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 50
(config-if-range)# exit
```
認証後にアクセスするネットワークのポートを指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

認証前 VLAN および認証後 VLAN に IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface vlan 10**
   (config-if)# ip address 192.168.10.254 255.255.255.0
   (config-if)# exit
   (config)# interface vlan 50
   (config-if)# ip address 192.168.50.254 255.255.255.0
   (config-if)# exit
   認証前 VLAN と認証後 VLAN に各 IP アドレスを設定します。

(c) 認証専用 IPv4 アクセスリストの設定

[設定のポイント]

認証前状態の端末から本装置の外部への通信を許可する認証専用 IPv4 アクセスリストを設定します。

[コマンドによる設定]

1. **(config)# ip access-list extended 100**
   (config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.10.254 eq bootps
   (config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
   (config-ext-nacl)# permit ip host 192.168.10.0 host 192.168.10.1
   (config-ext-nacl)# exit
   (config)# interface gigabitethernet 0/4
   (config-if)# authentication ip access-group 100
   (config-if)# authentication arp-relay
   (config-if)# exit
   認証前の端末から本装置内 DHCP サーバ向けの DHCP パケットと VLAN10 のデフォルトゲートウェイ（IP アドレス 192.168.10.1）へのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。さらに，ARP パケットを本装置の外部に転送させるよう設定します。

(d) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

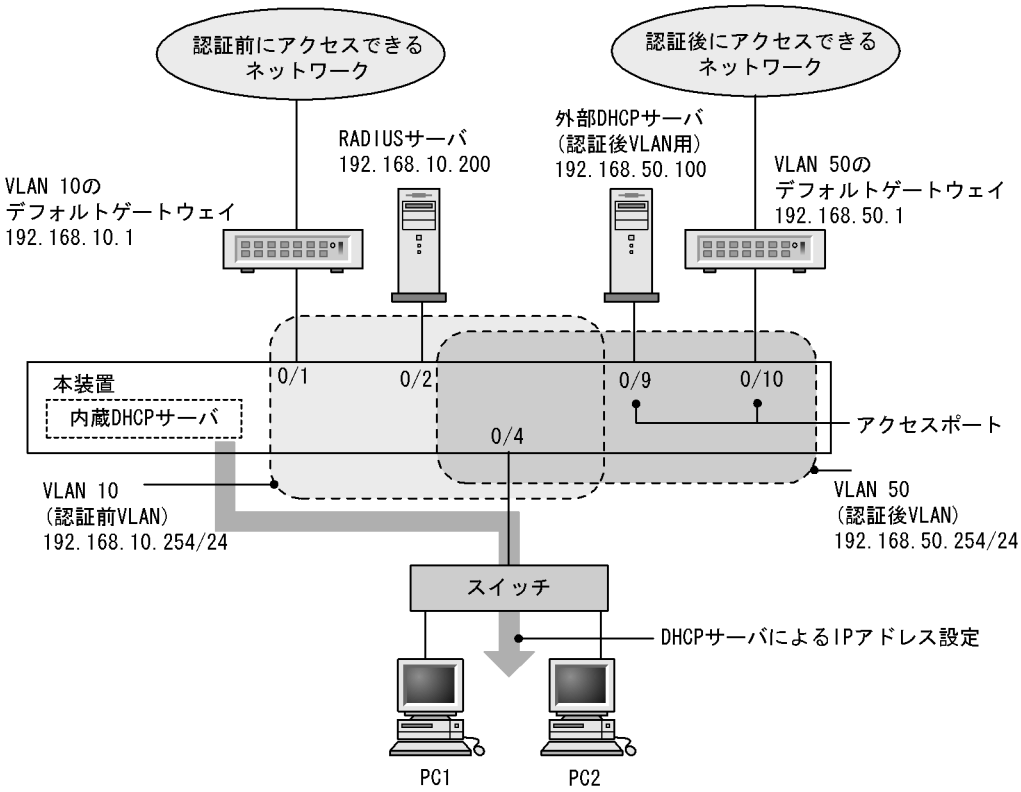
1. **(config)# web-authentication ip address 10.10.10.1**
   Web 認証専用の IP アドレス（IPv4 アドレス）を設定します。

2. **(config)# web-authentication system-auth-control**
   Web 認証を起動します。

(2) RADIUS 認証方式の基本的な設定

RADIUS 認証方式を使用する際の基本的な設定を次の図に示します。なお，端末の IP アドレスは，認証前は本装置内 DHCP サーバから配布し，認証後は外部 DHCP サーバから配布します。

図 9-5 ダイナミック VLAN モードの RADIUS 認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac native vlan 10
   (config-if)# web-authentication port
   (config-if)# exit
   認証を行う端末が接続されているポートに MAC VLAN と Web 認証を設定します。

2. **(config)# interface range gigabitethernet 0/9-10**
   (config-if-range)# switchport mode access
   (config-if-range)# switchport access vlan 50
   (config-if-range)# exit
   認証後にアクセスするネットワークのポートを指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

認証前 VLAN および認証後 VLAN に IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface vlan 10**
   (config-if)# ip address 192.168.10.254 255.255.255.0
   (config-if)# exit
   (config)# interface vlan 50
   (config-if)# ip address 192.168.50.254 255.255.255.0
   (config-if)# exit
   認証前 VLAN と認証後 VLAN に各 IP アドレスを設定します。

(c) 認証専用 IPv4 アクセスリストの設定

[設定のポイント]

認証前状態の端末から本装置の外部への通信を許可する認証専用 IPv4 アクセスリストを設定します。

[コマンドによる設定]

1. **(config)# ip access-list extended 100**
   (config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.10.254 eq bootps
   (config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
   (config-ext-nacl)# permit ip host 192.168.10.0 host 192.168.10.1
   (config-ext-nacl)# exit
   (config)# interface gigabitethernet 0/4
   (config-if)# authentication ip access-group 100
   (config-if)# authentication arp-relay
   (config-if)# exit
   認証前の端末から本装置内 DHCP サーバ向けの DHCP パケットと VLAN 10 のデフォルトゲートウェイ（IP アドレス 192.168.10.1）へのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。
   さらに，ARP パケットを本装置の外部に転送させるよう設定します。

(d) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

1. **(config)# web-authentication ip address 10.10.10.1**
   Web 認証専用の IP アドレス（IPv4 アドレス）を設定します。

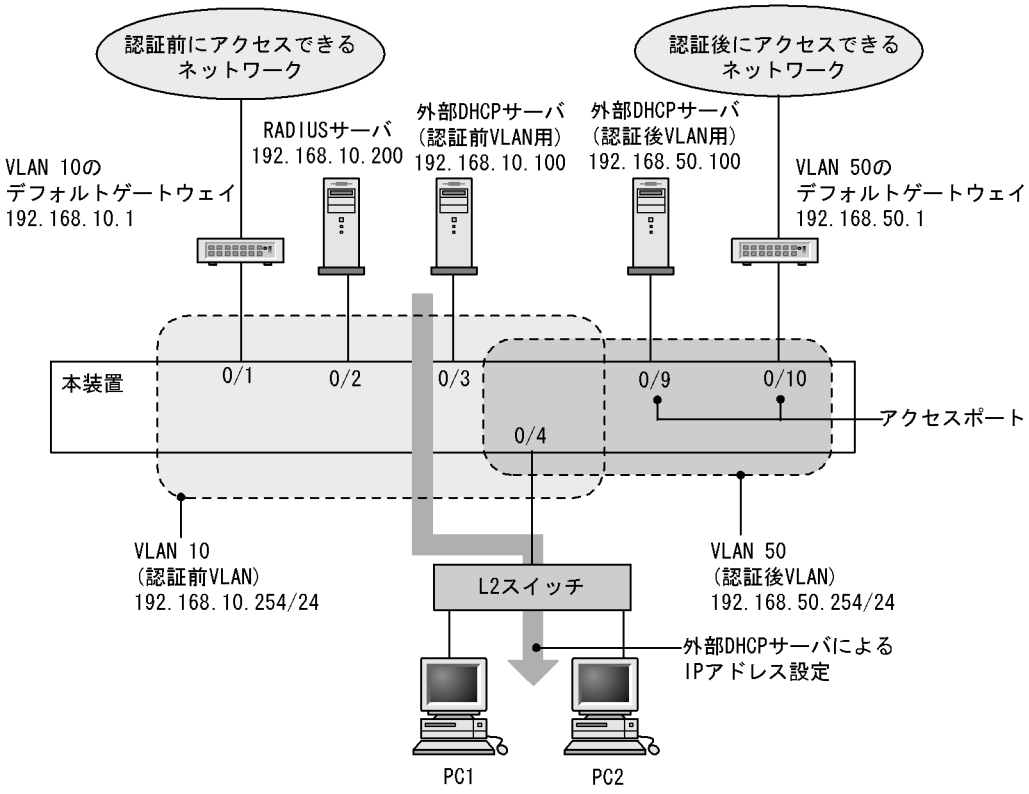
2. **(config)# aaa authentication web-authentication default group radius**
   (config)# radius-server host 192.168.10.200 key "webauth"
   ユーザ認証を RADIUS サーバで行うための IP アドレスと RADIUS 鍵を設定します。

3. **(config)# web-authentication system-auth-control**
   Web 認証を起動します。

(3) RADIUS 認証方式＋認証前に外部 DHCP サーバ使用時の設定

RADIUS 認証方式で認証前および認証後に，端末の IP アドレスをそれぞれの外部 DHCP サーバから配布する際の構成を次に示します。

図 9-6 ダイナミック VLAN モードの RADIUS 認証方式＋外部 DHCP サーバ使用時の構成



(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac native vlan 10
   (config-if)# web-authentication port
   (config-if)# exit
   認証を行う端末が接続されているポートに MAC VLAN と Web 認証を設定します。

2. **(config)# interface range gigabitethernet 0/9-10**
   (config-if-range)# switchport mode access
   (config-if-range)# switchport access vlan 50
   (config-if-range)# exit
   認証後にアクセスするネットワークのポートを指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

認証前 VLAN および認証後 VLAN に IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface vlan 10**
   (config-if)# ip address 192.168.10.254 255.255.255.0
   (config-if)# exit
   (config)# interface vlan 50
   (config-if)# ip address 192.168.50.254 255.255.255.0
   (config-if)# exit
   認証前 VLAN と認証後 VLAN に各 IP アドレスを設定します。

(c) 認証専用 IPv4 アクセスリストの設定

[設定のポイント]

認証前状態の端末から本装置の外部への通信を許可する認証専用 IPv4 アクセスリストを設定します。

[コマンドによる設定]

1. **(config)# ip access-list extended 100**
   (config-ext-nacl)# permit udp host 0.0.0.0 host 192.168.10.100 eq bootps
   (config-ext-nacl)# permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
   (config-ext-nacl)# permit ip host 192.168.10.0 host 192.168.10.1
   (config-ext-nacl)# exit
   (config)# interface gigabitethernet 0/4
   (config-if)# authentication ip access-group 100
   (config-if)# authentication arp-relay
   (config-if)# exit
   認証前の端末から外部 DHCP サーバ向けの DHCP パケットと VLAN 10 のデフォルトゲートウェイ（IP アドレス 192.168.10.1）へのアクセスを許可する認証専用 IPv4 アクセスリストを設定します。さらに，ARP パケットを本装置の外部に転送させるよう設定します。

(d) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

1. **(config)# web-authentication ip address 10.10.10.1**
   Web 認証専用の IP アドレス（IPv4 アドレス）を設定します。

2. **(config)# aaa authentication web-authentication default group radius**
   (config)# radius-server host 192.168.10.200 key "webauth"
   ユーザ認証を RADIUS サーバで行うための IP アドレスと RADIUS 鍵を設定します。

3. **(config)# web-authentication system-auth-control**

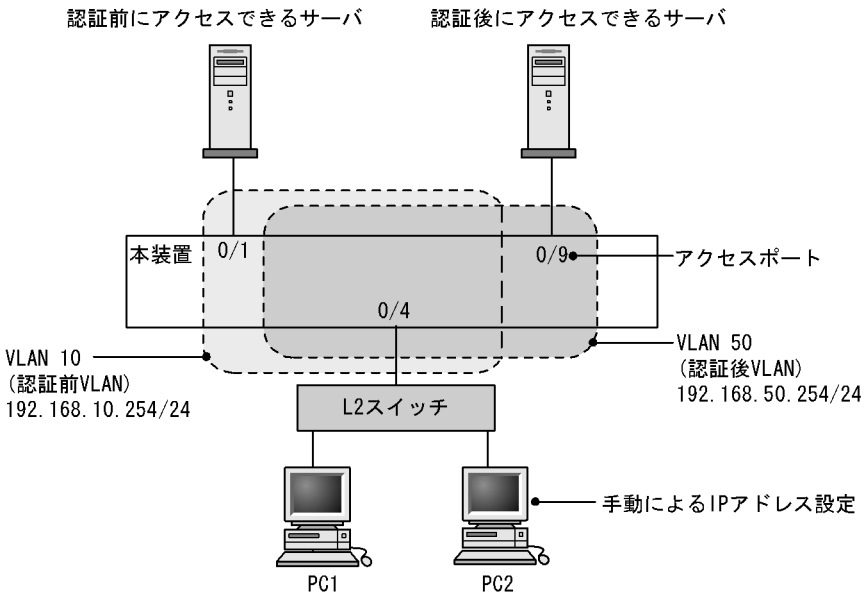
Web 認証を起動します。

9.1.4 レガシーモードのコンフィグレーション

(1) ローカル認証方式の基本的な設定

ローカル認証方式を使用する上での基本的な設定を次の図に示します。なお，端末（PC1，PC2）の IP アドレスは，端末側で認証前と認証後に手動で切り替えるものとします。

図 9-7 ローカル認証方式の構成例



(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac vlan 50
   (config-if)# switchport mac native vlan 10
   (config-if)# exit
   認証を行う端末が接続されているポートに認証前 VLAN と認証後 VLAN を指定します。

2. **(config)# interface gigabitethernet 0/9**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 50
   (config-if)# exit
   認証後に接続するサーバを接続するポートに認証後 VLAN を指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

認証前 VLAN および認証後 VLAN に IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface vlan 10**
   (config-if)# ip address 192.168.10.254 255.255.255.0
   (config-if)# exit
   (config)# interface vlan 50
   (config-if)# ip address 192.168.50.254 255.255.255.0
   (config-if)# exit
   認証前 VLAN と認証後 VLAN に各 IP アドレスを設定します。

(c) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

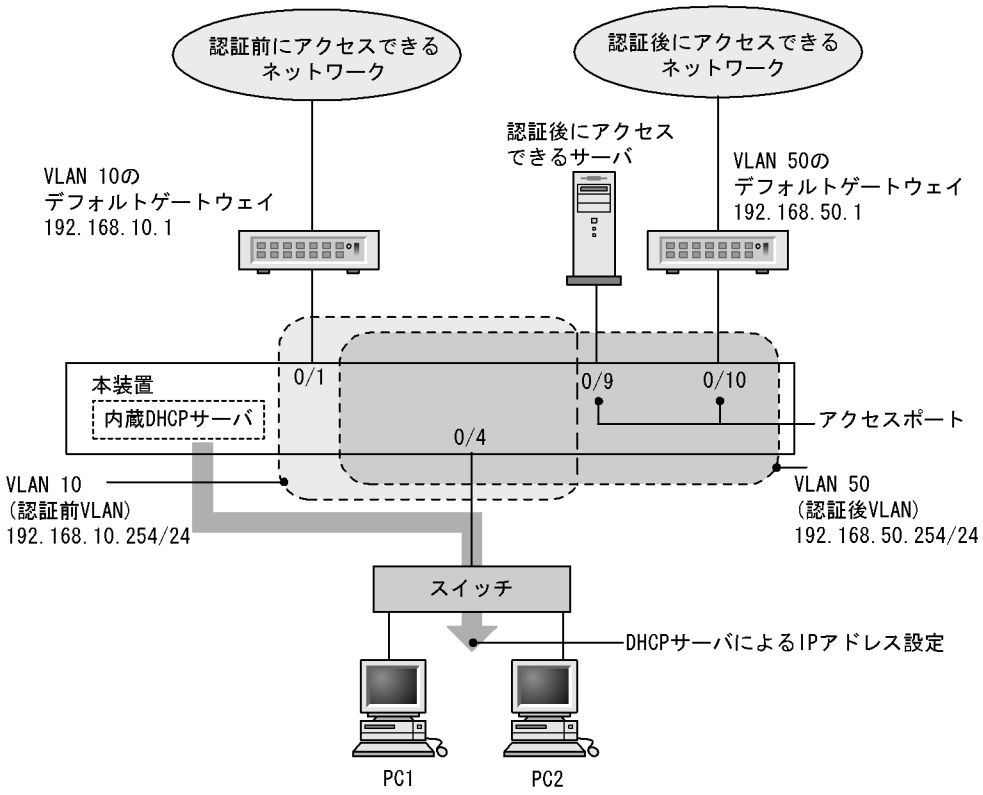
1. **(config)# web-authentication vlan 50**
   Web 認証の認証後 VLAN を設定するコンフィグレーションコマンドで VLAN ID を設定します。

2. **(config)# web-authentication system-auth-control**
   Web 認証を起動します。

(2) ローカル認証方式＋内蔵 DHCP サーバ使用時の構成

ローカル認証方式に内蔵 DHCP サーバを使用して Web 認証を構成した際の設定例を，次の図に示します。
なお，端末（PC1，PC2）の IP アドレスは，本装置内蔵の DHCP サーバ機能で割り当てるものとします。

図 9-8 ローカル認証方式＋内蔵 DHCP 使用時の構成例



認証前 VLAN と認証後 VLAN を設定し，DHCP サーバの設定を行ったあとに，Web 認証の設定をします。

(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac vlan 50
   (config-if)# switchport mac native vlan 10
   (config-if)# exit
   認証を行う端末が接続されているポートに認証前 VLAN と認証後 VLAN を指定します。

2. **(config)# interface range gigabitethernet 0/9-10**
   (config-if-range)# switchport mode access
   (config-if-range)# switchport access vlan 50
   (config-if-range)# exit
   認証後に接続するサーバを接続するポートに認証後 VLAN を指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

認証前 VLAN および認証後 VLAN に IP アドレスを設定します。

[コマンドによる設定]

1.
```
(config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# exit
```
認証前 VLAN と認証後 VLAN に各 IP アドレスを設定します。

(c) DHCP サーバの設定

[設定のポイント]

端末に IP アドレスを配布するための DHCP サーバを設定します。

[コマンドによる設定]

1.
```
(config)# service dhcp vlan 10
(config)# ip dhcp excluded-address 192.168.10.1
(config)# ip dhcp excluded-address 192.168.10.254
(config)# ip dhcp pool POOL10
(dhcp-config)# network 192.168.10.0/24
(dhcp-config)# lease 0 0 1
(dhcp-config)# default-router 192.168.10.1
(dhcp-config)# exit
```
DHCP サーバに認証前 VLAN 用の設定をします（端末認証に使用する IP アドレスの配布を設定します。デフォルトルータの IP アドレス 192.168.10.1 を設定します。）。

2.
```
(config)# service dhcp vlan 50
(config)# ip dhcp excluded-address 192.168.50.1
(config)# ip dhcp excluded-address 192.168.50.254
(config)# ip dhcp pool POOL50
(dhcp-config)# network 192.168.50.0/24
(dhcp-config)# lease 0 0 1
(dhcp-config)# default-router 192.168.50.1
(dhcp-config)# exit
```
DHCP サーバに認証後 VLAN 用の設定をします（認証された端末で使用する IP アドレスの配布を設定します。デフォルトルータの IP アドレス 192.168.50.1 を設定します。）。

(d) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

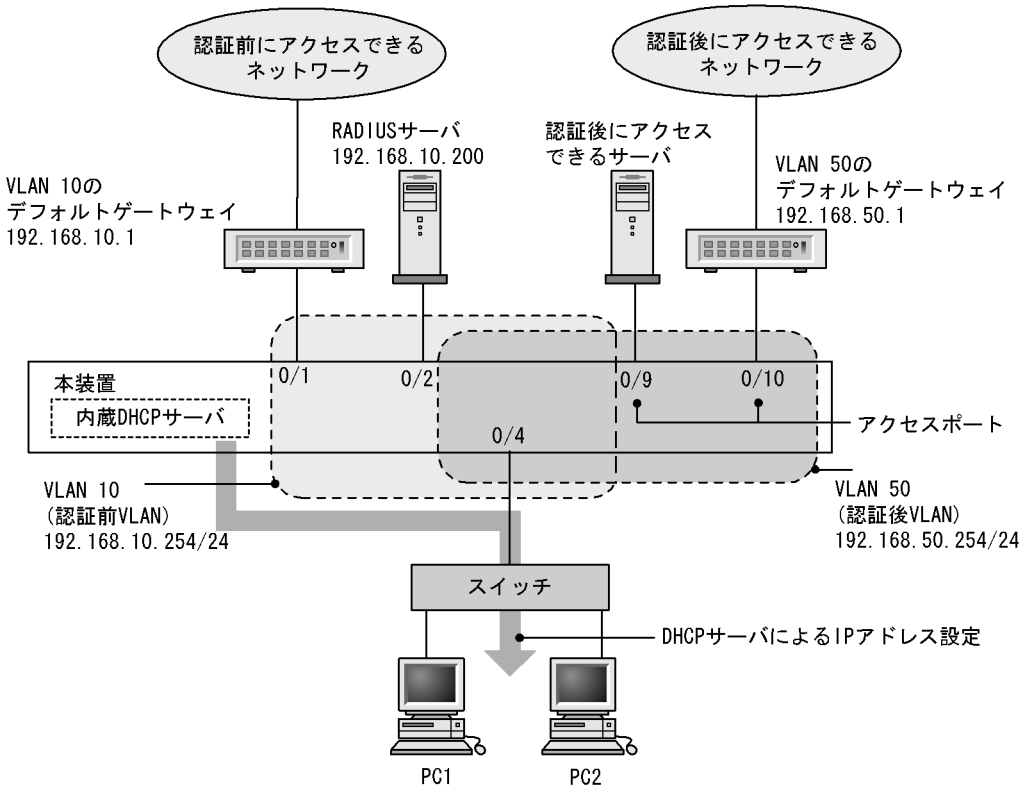
1. **(config)# web-authentication vlan 50**
   Web 認証の認証後 VLAN を設定するコンフィグレーションコマンドで VLAN ID を設定します。

2. **(config)# web-authentication system-auth-control**
   Web 認証を起動します。

(3) RADIUS 認証方式＋内蔵 DHCP サーバ使用時の構成

RADIUS 認証方式と内蔵 DHCP サーバを使用して Web 認証を構成した際の設定例を，次の図に示します。なお，端末（PC1，PC2）の IP アドレスは，本装置内蔵の DHCP サーバ機能で割り当てるものとします。

図 9-9 Web 認証の RADIUS 認証方式＋内蔵 DHCP 使用時の構成例



認証前 VLAN と認証後 VLAN を設定し，DHCP サーバの設定を行ったあとに，Web 認証の設定をします。

(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac vlan 50

```
(config-if)# switchport mac native vlan 10
(config-if)# exit
```
認証を行う端末が接続されているポートに認証前 VLAN と認証後 VLAN を指定します。

2.
```
(config)# interface range gigabitethernet 0/9-10
(config-if-range)# switchport mode access
(config-if-range)# switchport access vlan 50
(config-if-range)# exit
```
認証後に接続するサーバを接続するポートに認証後 VLAN を指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

認証前 VLAN および認証後 VLAN に IP アドレスを設定します。

[コマンドによる設定]

1.
```
(config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# exit
```
認証前 VLAN と認証後 VLAN に各 IP アドレスを設定します。

(c) DHCP サーバの設定

[設定のポイント]

端末に IP アドレスを配布するための DHCP サーバを設定します。

[コマンドによる設定]

1.
```
(config)# service dhcp vlan 10
(config)# ip dhcp excluded-address 192.168.10.1
(config)# ip dhcp excluded-address 192.168.10.254
(config)# ip dhcp pool POOL10
(dhcp-config)# network 192.168.10.0/24
(dhcp-config)# lease 0 0 1
(dhcp-config)# default-router 192.168.10.1
(dhcp-config)# exit
```
DHCP サーバに認証前 VLAN 用の設定をします（端末認証に使用する IP アドレス配布を設定します。デフォルトルータの IP アドレス 192.168.10.1 を設定します。）。

2.
```
(config)# service dhcp vlan 50
(config)# ip dhcp excluded-address 192.168.50.1
(config)# ip dhcp excluded-address 192.168.50.254
(config)# ip dhcp pool POOL50
(dhcp-config)# network 192.168.50.0/24
(dhcp-config)# lease 0 0 1
```

```
(dhcp-config)# default-router 192.168.50.1
(dhcp-config)# exit
```

DHCP サーバに認証後 VLAN 用の設定をします（認証された端末で使用する IP アドレスの配布を設定します。デフォルトルータの IP アドレス 192.168.50.1 を設定します。）。

（d） Web 認証の設定

［設定のポイント］

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

［コマンドによる設定］

1.
```
(config)# web-authentication vlan 50
```
Web 認証の認証後 VLAN を設定するコンフィグレーションコマンドで VLAN ID を設定します。

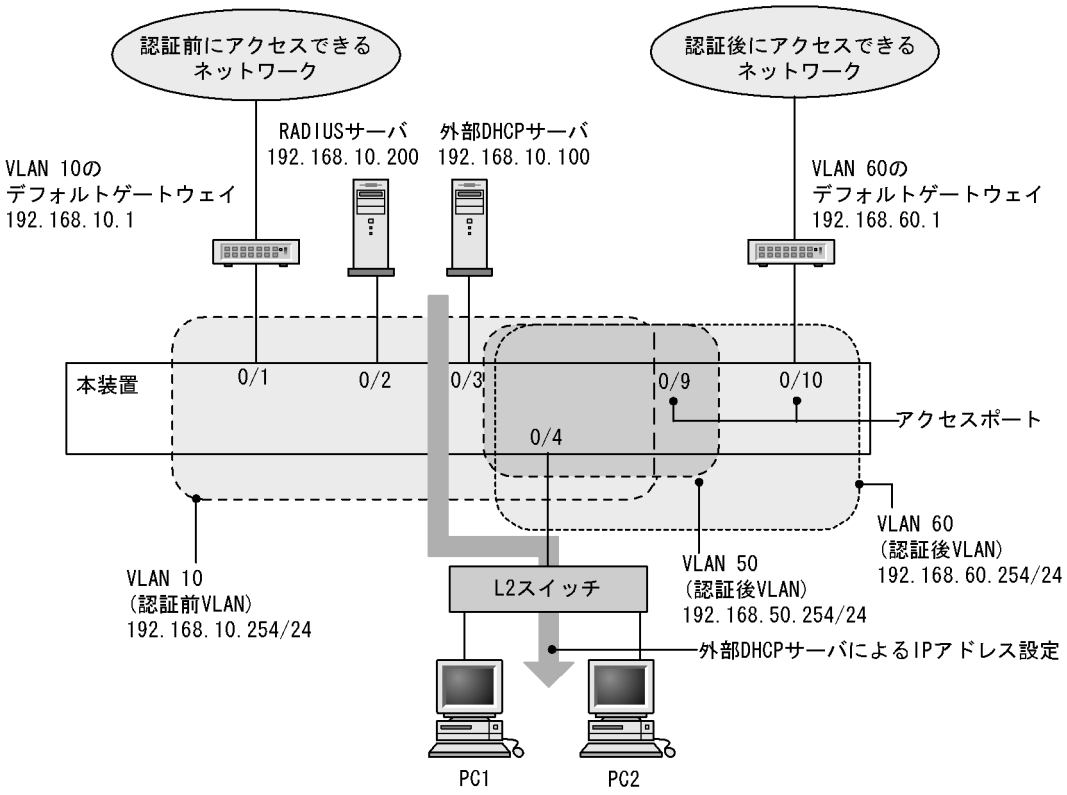
2.
```
(config)# aaa authentication web-authentication default group radius
(config)# radius-server host 192.168.10.200 key "webauth"
```
ユーザ認証を RADIUS サーバで行うための IP アドレスと RADIUS 鍵を設定します。

3.
```
(config)# web-authentication system-auth-control
```
Web 認証を起動します。

（4） RADIUS 認証方式＋外部 DHCP サーバ＋複数の認証後 VLAN 使用時の構成

RADIUS 認証方式と外部 DHCP サーバを使用し，複数の認証後 VLAN を設定する場合の Web 認証設定例を次の図に示します。なお，端末（PC1，PC2）の IP アドレスは，外部 DHCP サーバによって割り当てるものとします。

図 9-10 Web 認証の RADIUS 認証方式＋外部 DHCP サーバ＋複数認証後 VLAN 使用時の構成例



認証前 VLAN と認証後 VLAN を設定し，Web 認証の設定をします。

(a) 認証ポートの設定

[設定のポイント]

Web 認証で使用するポートを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# switchport mode mac-vlan
   (config-if)# switchport mac vlan 50,60
   (config-if)# switchport mac native vlan 10
   (config-if)# exit
   認証を行う端末が接続されているポートに認証前 VLAN と認証後 VLAN を指定します。

2. **(config)# interface gigabitethernet 0/9**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 50
   (config-if)# exit
   認証後に接続するサーバを接続するポートに認証後 VLAN を指定します。

3. **(config)# interface gigabitethernet 0/10**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 60

```
(config-if)# exit
```
認証後に接続するサーバを接続するポートに認証後 VLAN を指定します。

(b) VLAN インタフェースに IP アドレスを設定

[設定のポイント]

認証前 VLAN および認証後 VLAN に IP アドレスを設定します。

[コマンドによる設定]

1.
```
(config)# interface vlan 10
(config-if)# ip address 192.168.10.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 50
(config-if)# ip address 192.168.50.254 255.255.255.0
(config-if)# exit
(config)# interface vlan 60
(config-if)# ip address 192.168.60.254 255.255.255.0
(config-if)# exit
```
認証前 VLAN と認証後 VLAN に各 IP アドレスを設定します。

(c) Web 認証の設定

[設定のポイント]

Web 認証のコンフィグレーションコマンドを設定して Web 認証を有効にします。

[コマンドによる設定]

1.
```
(config)# web-authentication vlan 50
(config)# web-authentication vlan 60
```
Web 認証の認証後 VLAN を設定するコンフィグレーションコマンドで VLAN ID を設定します。

2.
```
(config)# aaa authentication web-authentication default group radius
(config)# radius-server host 192.168.10.200 key "webauth"
```
ユーザ認証を RADIUS サーバで行うための IP アドレスと RADIUS 鍵を設定します。

3.
```
(config)# web-authentication system-auth-control
```
Web 認証を起動します。

9.1.5 Web 認証のパラメータ設定

Web 認証で可能なパラメータ設定を説明します。

(1) 認証最大時間の設定

[設定のポイント]

認証済みの端末を強制的にログアウトする時間を設定します。

[コマンドによる設定]

1. **(config)# web-authentication max-timer 60**
   強制ログアウト時間を 60 分に設定します。

(2) 認証ユーザ数の設定（固定 VLAN モード）

[設定のポイント]

Web 認証の固定 VLAN モードで認証できるユーザ数を設定します。

[コマンドによる設定]

1. **(config)# web-authentication static-vlan max-user 100**
   Web 認証の固定 VLAN モードで認証できるユーザ数を 100 ユーザに設定します。

(3) 認証ユーザ数の設定（ダイナミック VLAN モード，レガシーモード）

[設定のポイント]

Web 認証のダイナミック VLAN モードまたはレガシーモードで認証できるユーザ数を設定します。

[コマンドによる設定]

1. **(config)# web-authentication max-user 5**
   Web 認証で認証できるユーザ数を 5 ユーザに設定します。

(4) RADIUS サーバの設定

[設定のポイント]

RADIUS 認証方式で使用する RADIUS サーバを設定します。

[コマンドによる設定]

1. **(config)# aaa authentication web-authentication default group radius**
   RADIUS サーバでユーザ認証を行うように設定します。

[注意事項]

各 RADIUS サーバの radius-server コマンドで設定された応答待ち時間（再送回数×応答タイムアウト時間）の合計が 60 秒を超える場合，RADIUS サーバへ認証要求している途中で認証失敗となることがあります。なお，Web 認証で使用する radius-server コマンドの設定は，ログイン認証，コマンド承認，および IEEE802.1X でも共通して使用するため，応答待ち時間の設定には注意してください。

(5) アカウンティングの設定

[設定のポイント]

Web 認証のアカウンティング集計を行うよう設定します。

[コマンドによる設定]

1. **(config)# aaa accounting web-authentication default start-stop group radius**
   RADIUS サーバにアカウンティング集計を行うよう設定します。

（6）Web 認証専用 IP アドレスの設定（固定 VLAN モード，ダイナミック VLAN モード）

[設定のポイント]

Web 認証専用の IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# web-authentication ip address 10.10.10.1**
   Web 認証専用の IP アドレス（10.10.10.1）を設定します。

[注意事項]

- 設定を行った場合は，運用コマンド restart web-authentication web-server で Web サーバを再起動してください。認証途中のユーザは再度ログイン操作が必要です。
- レガシーモードの状態（web-authentication port コマンドが設定されていない状態）で，本コマンドを設定したあとに web-authentication port コマンドを設定した場合は，運用コマンド restart web-authentication web-server で Web サーバを再起動してください。

（7）Web 認証専用 IP アドレスと FQDN の設定（固定 VLAN モード，ダイナミック VLAN モード）

[設定のポイント]

Web 認証専用の IP アドレスと FQDN を設定します。

[コマンドによる設定]

1. **(config)# web-authentication ip address 10.10.10.1 fqdn host.example.com**
   Web 認証専用の IP アドレス（10.10.10.1）と FQDN（host.example.com）を設定します。

[注意事項]

- 設定を行った場合は，運用コマンド restart web-authentication web-server で Web サーバを再起動してください。認証途中のユーザは再度ログイン操作が必要です。
- レガシーモードの状態（web-authentication port コマンドが設定されていない状態）で，本コマンドを設定したあとに web-authentication port コマンドを設定した場合は，運用コマンド restart web-authentication web-server で Web サーバを再起動してください。

（8）URL リダイレクト機能の無効設定（固定 VLAN モード，ダイナミック VLAN モード）

[設定のポイント]

Web 認証の URL リダイレクト機能を無効に設定します。

[コマンドによる設定]

1. **(config)# no web-authentication redirect enable**
   Web 認証の URL リダイレクト機能を無効にします。

[注意事項]

設定を行った場合は，運用コマンド restart web-authentication web-server で Web サーバを再起動してください。認証途中のユーザは再度ログイン操作が必要です。

(9) URL リダイレクト機能時のログイン操作プロトコルの設定（固定 VLAN モード，ダイナミック VLAN モード）

[設定のポイント]

Web 認証の URL リダイレクト機能時にログインを操作させるプロトコルを設定します。

[コマンドによる設定]

1. **(config)# web-authentication redirect-mode https**
   Web 認証の URL リダイレクト機能で https を用います。

[注意事項]

設定を行った場合は，運用コマンド restart web-authentication web-server で Web サーバを再起動してください。認証途中のユーザは再度ログイン操作が必要です。

(10) syslog サーバへの出力設定

[設定のポイント]

認証結果と動作ログを syslog サーバに出力する設定をします。

[コマンドによる設定]

1. **(config)# web-authentication logging enable**
   (config)# logging event-kind aut
   Web 認証の結果と動作ログを syslog サーバに出力する設定をします。

(11) 接続監視機能の設定（固定 VLAN モード）

[設定のポイント]

認証済み端末の動作を監視する接続監視機能を設定します。

[コマンドによる設定]

1. **(config)# web-authentication logout polling enable**
   接続監視機能を有効に設定します。

2. **(config)# web-authentication logout polling interval 300**
   動作監視パケットの送出時間間隔を 300 秒に設定します。

3. **(config)# web-authentication logout polling retry-interval 10**
   動作監視パケットの再送出時間間隔を 10 秒に設定します。

4. **(config)# web-authentication logout polling count 5**
   動作監視パケットの送出回数を 5 回に設定します。

(12) 接続監視機能の無効設定（固定 VLAN モード）

[設定のポイント]

認証済み端末の動作を監視する接続監視機能を無効に設定します。

[コマンドによる設定]

1. **(config)# no web-authentication logout polling enable**
   接続監視機能を無効に設定します。

(13) Web サーバへのアクセスポート番号設定

[設定のポイント]

Web 認証で使用している Web サーバのサービスポート番号を設定します（デフォルトの http=80 番，https=443 番以外に追加する場合に使用します）。
また，OAN と共存する場合は，OAN が使用するサービスポート番号（832 と 9698）を設定します。この場合，OAN が使用するサービスポート番号では Web 認証のログイン操作およびログアウト操作はできません。

[コマンドによる設定]

1. **(config)# web-authentication web-port http 8080**
   Web サーバの http ポートとして 80 番のほかに 8080 番も設定します。

2. **(config)# web-authentication web-port https 8443**
   Web サーバの https ポートとして 443 番のほかに 8443 番も設定します。

[注意事項]

設定を行った場合は，運用コマンド restart web-authentication web-server で Web サーバを再起動してください。認証途中のユーザは再度ログイン操作が必要です。

(14) 認証成功後の URL 設定

[設定のポイント]

認証成功後に端末がアクセスする URL を設定します。

[コマンドによる設定]

1. **(config)# web-authentication jump-url "http://www.example.com/"**
   認証成功後に http://www.example.com/ の画面を表示させます。

9.1.6 認証除外の設定方法

Web 認証で認証対象外とするための設定を説明します。

(1) 固定 VLAN モードの認証除外ポートの設定

固定 VLAN モードで，認証しないで通信を許可するポートを次のように設定します。

[設定のポイント]

認証を除外するポートに対しては，認証ポートを設定しません。

[コマンドによる設定]

1. **(config)# vlan 10**
   (config-vlan)# state active
   (config-vlan)# exit
   (config)# interface gigabitethernet 0/4

```
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# web-authentication port
(config-if)# exit
(config)# interface gigabitethernet 0/10
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# exit
```

固定 VLAN モードで扱う VLAN ID 10 を設定したポート 0/4 は認証対象ポートとして設定します。また，ポート 0/10 には認証しないで通信を許可する設定をします。

(2) 固定 VLAN モードの認証除外端末の設定

固定 VLAN モードで，認証しないで通信を許可する端末の MAC アドレスを次のように設定します。

[設定のポイント]

認証を除外する端末の MAC アドレスを MAC アドレステーブルに登録します。

[コマンドによる設定]

1.
```
(config)# vlan 10
(config-vlan)# exit
(config)# mac-address-table static 0012.e212.3456 vlan 10 interface
gigabitethernet 0/10
```

VLAN ID 10 のポート 0/10 に，認証しないで通信を許可する端末の MAC アドレスを設定します。

(3) ダイナミック VLAN モードの認証除外ポートの設定

ダイナミック VLAN モードで，認証しないで通信を許可するポートを次のように設定します。

[設定のポイント]

認証を除外するポートをアクセスポートとして設定し，認証対象ポートを設定しません。

[コマンドによる設定]

1.
```
(config)# vlan 50 mac-based
(config-vlan)# state active
(config-vlan)# exit
(config)# interface gigabitethernet 0/10
(config-if)# switchport mode access
(config-if)# switchport access vlan 50
(config-if)# exit
```

MAC VLAN ID 50 のポート 0/10 に対して，認証しないで通信を許可する設定をします。

(4) ダイナミック VLAN モードの認証除外端末の設定

ダイナミック VLAN モードで，認証しないで通信を許可する端末の MAC アドレスを次のように設定します。

[設定のポイント]

認証を除外する端末の MAC アドレスを，MAC VLAN と MAC アドレステーブルに登録します。

[コマンドによる設定]

1. **(config)# vlan 50 mac-based**
   (config-vlan)# mac-address 0012.e212.3456
   (config-vlan)# exit
   (config)# mac-address-table static 0012.e212.3456 vlan 50 interface gigabitethernet 0/10
   MAC VLAN ID 50 のポート 0/10 に，認証しないで通信を許可する端末の MAC アドレスを設定します。

(5) レガシーモードの認証除外ポートの設定

レガシーモードで，認証しないで通信を許可するポートを次のように設定します。

[設定のポイント]

認証を除外するポートをアクセスポートとして設定します。

[コマンドによる設定]

1. **(config)# vlan 50 mac-based**
   (config-vlan)# state active
   (config-vlan)# exit
   (config)# interface gigabitethernet 0/10
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 50
   (config-if)# exit
   MAC VLAN ID 50 のポート 0/10 に対して，認証しないで通信を許可する設定をします。

(6) レガシーモードの認証除外端末の設定

レガシーモードで，認証しないで通信を許可する端末の MAC アドレスを次のように設定します。

[設定のポイント]

認証を除外する端末の MAC アドレスを MAC VLAN に登録します。

[コマンドによる設定]

1. **(config)# vlan 50 mac-based**
   (config-vlan)# mac-address 0012.e212.3456
   (config-vlan)# exit
   VLAN ID 50 の MAC VLAN に，認証しないで通信を許可する端末の MAC アドレスを設定します。

9.2 オペレーション

9.2.1 運用コマンド一覧

Web 認証の運用コマンド一覧を次の表に示します。

表 9-2 運用コマンド一覧

コマンド名	説明
set web-authentication user	Web 認証で使用するユーザ ID を追加します。
set web-authentication passwd	登録したユーザのパスワードを変更します。
set web-authentication vlan	登録したユーザの VLAN ID を変更します。
remove web-authentication user	登録したユーザ ID を削除します。
commit web-authentication	追加，変更した内容を内蔵 Web 認証 DB に反映します。
store web-authentication	内蔵 Web 認証 DB のバックアップファイルを作成します。
load web-authentication	バックアップファイルから内蔵 Web 認証 DB を復元します。
show web-authentication user	内蔵 Web 認証 DB の登録内容，または追加，変更途中の情報を表示します。
clear web-authentication auth-state	認証済みユーザの強制ログアウトを行います。
show web-authentication login	認証済のアカウントログを表示します。
show web-authentication	Web 認証のコンフィグレーションを表示します。
show web-authentication statistics	Web 認証の統計情報を表示します。
clear web-authentication statistics	統計情報をクリアします。
show web-authentication logging	Web 認証の動作ログを表示します。
clear web-authentication logging	Web 認証の動作ログをクリアします。
set web-authentication html-files	指定された Web 認証画面ファイルを登録します。
clear web-authentication html-files	登録した Web 認証画面ファイルを削除します。
show web-authentication html-files	登録した Web 認証画面ファイルのファイル名，ファイルサイズと登録日時を表示します。
clear web-authentication dead-interval-timer	dead interval 機能による 2 台目以降の RADIUS サーバへのアクセスから，1 台目の RADIUS サーバへのアクセスに戻します。
restart web-authentication	Web 認証プログラムを再起動します。
dump protocols web-authentication	Web 認証のダンプ情報を収集します。

9.2.2 Web 認証の設定情報表示

show web-authentication コマンドで Web 認証の設定情報が表示されます。

(1) 固定 VLAN モードで，認証方式が RADIUS 認証の場合

図 9-11 Web 認証の設定情報表示（固定 VLAN モードの RADIUS 認証）

```
# show web-authentication
Date 2008/10/17 10:52:49 UTC
web-authentication Information:
   Authentic-mode   : Static-VLAN
   Authentic-method : RADIUS        Accounting-state : disable
   Dead-interval    : 10
          Max-timer : 60                  Max-user  : 256
         VLAN Count : -                 Auto-logout : -
   Syslog-send      : enable
   Alive-detection  : enable
              timer : 60    interval-timer : 3     count : 3
   URL-redirect     : enable    Protocol : http
   Jump-URL         : http://www.example.com/
   Web-IP-address   : 10.10.10.1
   FQDN             : aaa.example.com
   Web-port         : http  : 80, 8080       https : 443, 8443
   ARP-relay Port   : 0/1-2
   Force-Authorized : disable
   Auth-max-user    : 1024

         Port          :    0/1
         VLAN ID       :    5,10,15
         Access-list-No:    100
         Max-user      :    64

         Port          :    0/2
         VLAN ID       :    15-16
         Access-list-No:    100
         Max-user      :    64
```

(2) ダイナミック VLAN モードで，認証方式がローカル認証の場合

図 9-12 Web 認証の設定情報表示（ダイナミック VLAN モードのローカル認証）

```
# show web-authentication
Date 2008/10/17 10:52:49 UTC
web-authentication Information:
   Authentic-mode   : Dynamic-VLAN
   Authentic-method : Local         Accounting-state : disable
   Dead-interval    : 10
          Max-timer : 60                  Max-user  : 256
         VLAN Count : -                 Auto-logout : disable
   Syslog-send      : enable
   URL-redirect     : enable    Protocol : http
   Jump-URL         : http://www.example.com/
   Web-IP-address   : 192.168.1.1
   FQDN             : aaa.example.com
   Web-port         : http  : 80, 8080       https : 443, 8443
   ARP-relay Port   : 0/10,12
   Force-Authorized : enable
   Auth-max-user    : 1024

         Port          :    0/10
         VLAN ID       :    1000,1500
         Native VLAN   :    10
         Forceauth VLAN:    1000
         Access-list-No:    100
         Max-user      :    64

         Port          :    0/12
         VLAN ID       :    1000,1500
         Native VLAN   :    10
         Forceauth VLAN:    1000
         Access-list-No:    100
         Max-user      :    64
```

(3) ダイナミック VLAN モードで，認証方式が RADIUS 認証の場合

図 9-13 Web 認証の設定情報表示（ダイナミック VLAN モードの RADIUS 認証）

```
# show web-authentication
Date 2008/10/17 10:52:49 UTC
web-authentication Information:
   Authentic-mode   : Dynamic-VLAN
   Authentic-method : RADIUS        Accounting-state : enable
   Dead-interval    : 10
          Max-timer : 60                  Max-user  : 256
         VLAN Count : -                 Auto-logout : disable
   Syslog-send      : enable
   URL-redirect     : enable    Protocol : http
   Jump-URL         : http://www.example.com/
   Web-IP-address   : 192.168.1.1
   FQDN             : aaa.example.com
   Web-port         : http  : 80, 8080       https : 443, 8443
   ARP-relay Port   : 0/10,12
   Force-Authorized : enable
   Auth-max-user    : 1024

         Port           :    0/10
         VLAN ID        :    1000,1500
         Native VLAN    :    10
         Forceauth VLAN:     1000
         Access-list-No:     100
         Max-user       :    256

         Port           :    0/12
         VLAN ID        :    1000,1500
         Native VLAN    :    10
         Forceauth VLAN:     -
         Access-list-No:     100
         Max-user       :    256
```

(4) レガシーモードで VLAN が登録されていて，認証方式がローカル認証の場合

図 9-14 Web 認証の設定情報表示（ローカル認証）

```
# show web-authentication
Date 2008/10/17 10:52:49 UTC
web-authentication Information:
   Authentic-mode   : Legacy
   Authentic-method : Local         Accounting-state : disable
          Max-timer : 60                  Max-user  : 256
         VLAN Count : 16                Auto-logout : disable
   Syslog-send      : enable
   Jump-URL         : http://www.example.com/
   Web-port         : http  : 80             https : 443

VLAN Information:
            VLAN ID :    5,10,15,20,25,30,35,40,1000-1007
```

(5) レガシーモードで VLAN が登録されていて，認証方式が RADIUS 認証の場合

図 9-15 Web 認証の設定情報表示（RADIUS 認証）

```
# show web-authentication
Date 2008/10/17 10:52:49 UTC
web-authentication Information:
   Authentic-mode   : Legacy
   Authentic-method : RADIUS        Accounting-state : disable
          Max-timer : 60                  Max-user  : 256
         VLAN Count : 16                Auto-logout : disable
   Syslog-send      : enable
   Jump-URL         : http://www.example.com/
   Web-port         : http  : 80             https : 443

VLAN Information:
            VLAN ID :    5,10,15,20,25,30,35,40,1000-1007
```

9.2.3 Web 認証の状態表示

show web-authentication statistics コマンドで Web 認証の状態および RADIUS との通信状況が表示されます。

図 9-16 Web 認証の表示

```
# show web-authentication statistics
Date 2008/10/17 11:10:49 UTC
web-authentication Information:
  Authentication Request Total :         100
  Authentication Current Count :          10
  Authentication Error Total   :          30
  Force Authorized Count       :          10
RADIUS web-authentication Information:
[RADIUS frames]
           TxTotal   :        10  TxAccReq  :        10  TxError   :         0
           RxTotal   :        30  RxAccAccpt:        10  RxAccRejct:        10
                                  RxAccChllg:        10  RxInvalid :         0
Account web-authentication Information:
[Account frames]
           TxTotal   :        10  TxAccReq  :        10  TxError   :         0
           RxTotal   :        20  RxAccResp :        10  RxInvalid :         0
Port Information
  Port     User-count
   0/10       5/ 256
   0/12       5/1024
```

9.2.4 Web 認証の認証状態表示

show web-authentication login コマンドで Web 認証の認証状態が表示されます。

(1) 固定 VLAN モードの場合

図 9-17 Web 認証の認証状態表示（固定 VLAN モード）

```
# show web-authentication login
Date 2008/10/17 10:52:49 UTC
Total user counts:2
F Username
  VLAN    MAC address      Port  IP address
  Login time               Limit time
  USER00123456789
     3    0012.e200.9166   0/5   192.168.0.1
  2008/10/17 09:58:04 UTC  00:10:20
* USER01
  4094    0012.e268.7527   0/6   192.168.1.10
  2008/10/17 10:10:23 UTC  00:20:35
```

(2) ダイナミック VLAN モードの場合

図 9-18 Web 認証の認証状態表示（ダイナミック VLAN モード）

```
# show web-authentication login
Date 2008/10/17 10:52:49 UTC
Total user counts:2
F Username
  VLAN    MAC address      Login time               Limit time
  USER00123456789
     3    0012.e200.9166   2008/10/17 09:58:04 UTC  00:10:20
* USER01
  4094    0012.e268.7527   2008/10/17 10:10:23 UTC  00:20:35
```

(3) レガシーモードの場合

図 9-19 Web 認証の認証状態表示（レガシーモード）

```
# show web-authentication login
Date 2008/10/17 10:52:49 UTC
Total user counts:2
Username
VLAN    MAC address      Login time               Limit time
USER00123456789
   3    0012.e200.9166   2008/10/17 09:58:04 UTC  00:10:20
USER01
4094    0012.e268.7527   2008/10/17 10:10:23 UTC  00:20:35
```

9.2.5 内蔵 Web 認証 DB の作成

Web 認証システムの環境設定およびコンフィグレーションの設定が完了したあとに，内蔵 Web 認証 DB の作成を行います。また，すでに内蔵 Web 認証 DB に登録されているユーザ情報の修正を行います。

(1) ユーザの登録

認証対象のユーザごとに set web-authentication user コマンドで，ユーザ ID，パスワード，VLAN ID を登録します。次の例では，USER01 ～ USER05 の 5 ユーザ分を登録します。

[コマンド入力]

```
# set web-authentication user USER01 PAS0101 100
# set web-authentication user USER02 PAS0200 100
# set web-authentication user USER03 PAS0300 100
# set web-authentication user USER04 PAS0320 100
# set web-authentication user USER05 PAS0400 100
```

(2) ユーザ情報変更と削除

登録済みユーザのパスワード，VLAN ID の変更およびユーザの削除は次の手順で行います。

(a) パスワード変更

[コマンド入力]

```
# set web-authentication passwd USER01 PAS0101 PPP4321
```

ユーザ ID（USER01）のパスワードを PAS0101 から PPP4321 に変更します。

```
# set web-authentication passwd USER02 PAS0200 BBB1234
```

ユーザ ID（USER02）のパスワードを PAS0200 から BBB1234 に変更します。

(b) VLAN ID 変更

[コマンド入力]

```
# set web-authentication vlan BBB1234 200
```

ユーザ ID（BBB1234）の VLAN ID を 200 に変更します。

(c) ユーザ削除

[コマンド入力]

```
# remove web-authentication user PPP4321
```

ユーザ ID（PPPP4321）を削除します。

(3) 内蔵 Web 認証 DB への反映

set web-authentication コマンドおよび remove web-authentication コマンドで登録・変更したユーザ情報を内蔵 Web 認証 DB に反映します。

[コマンド入力]

```
# commit web-authentication
```

9.2.6 内蔵 Web 認証 DB のバックアップ

内蔵 Web 認証 DB のバックアップおよびバックアップファイルからの復元を示します。

(1) 内蔵 Web 認証 DB のバックアップ

内蔵 Web 認証 DB から store web-authentication コマンドでバックアップファイル（次の例では backupfile）を作成します。

[コマンド入力]

```
# store web-authentication backupfile
Backup web-authentication user data.  Are you sure? (y/n): y
#
```

(2) 内蔵 Web 認証 DB の復元

バックアップファイル（次の例では backupfile）から load web-authentication コマンドで内蔵 Web 認証 DB を作成します。

[コマンド入力]

```
# load web-authentication backupfile
Restore web-authentication user data.  Are you sure? (y/n): y
#
```

9.2.7 Web 認証画面の登録

Web 認証画面の登録は次の手順で行います。

1. **各 Web 認証画面のファイルを外部装置（PC など）で作成します。**
2. **本装置へログインし，カレントディレクトリに Web 認証画面を格納するディレクトリを作成します。**
3. **画面ファイルを 2. で作成したディレクトリ配下に，ファイル転送または MC 経由で格納します。**
4. set web-authentication html-files **コマンドで Web 認証画面を登録します。**

図 9-20 Web 認証画面の登録

```
# mkdir docs                                        …1

# set web-authentication html-files docs
Would you wish to install new html-files ? (y/n):y
executing...
Install complete.
#
```

1. ディレクトリ docs を作成し，配下に，登録するファイルを置きます。

9.2.8 登録した Web 認証画面の削除

set web-authentication html-files コマンドで登録した Web 認証画面を clear web-authentication html-files コマンドで削除します。

図 9-21 Web 認証画面の削除

```
# clear web-authentication html-files
Would you wish to clear registered html-files and initialize? (y/n):y
Clear complete.
#
```

9.2.9 Web 認証画面の情報表示

show web-authentication html-files コマンドで，登録した Web 認証画面の情報を表示します。

図 9-22 Web 認証画面の情報表示

```
# show web-authentication html-files
Date 2009/04/15 10:00:10 UTC
TOTAL SIZE      :       62976
-------------------------------------------------
                        SIZE         DATE
login.html      :        2049      2009/04/10 14:05
loginProcess.html        2002      2009/04/10 14:05
loginOK.html    :        1046      2009/04/10 14:05
loginNG.html    :         985      2009/04/10 14:05
logout.html     :         843      2009/04/10 14:05
logoutOK.html   :         856      2009/04/10 14:05
logoutNG.html   :         892      2009/04/10 14:05
webauth.msg     :         104      2009/04/10 14:05
favicon.ico     :         199      2009/04/10 14:05
the other files :       54000      2009/04/10 14:05
#
```

9.2.10 dead interval 機能による RADIUS サーバアクセスを 1 台目の RADIUS サーバに戻す

1 台目の RADIUS サーバが無応答になり，dead interval 機能によって，2 台目以降の RADIUS サーバへのアクセスに切り替わった場合，コンフィグレーションコマンド authentication radius-server dead-interval で設定された時間を待たないで最初の RADIUS サーバへのアクセスに戻すには，clear web-authentication dead-interval-timer コマンドを実行します。

図 9-23 1 台目の RADIUS サーバへの切り替え

```
# clear web-authentication dead-interval-timer
#
```

9.3 Web 認証画面作成手引き

Web 認証画面入れ替え機能で入れ替えができる画面と対応するファイル名を次に示します。

- ログイン画面（ファイル名：login.html）
- ログアウト画面（ファイル名：logout.html）
- ログイン成功画面（ファイル名：loginOK.html）
- ログイン失敗画面（ファイル名：loginNG.html）
- ログアウト完了画面（ファイル名：logoutOK.html）
- ログアウト失敗画面（ファイル名：logoutNG.html）
- Reply-Message 表示画面（ファイル名：loginProcess.html）

各 Web 認証画面ファイルは HTML 形式で作成してください。

HTML 上には，JavaScript のようにクライアント端末上だけで動作する言語は使用可能ですが，サーバへアクセスするような言語は使用できません。また，perl などの CGI も指定しないでください。

ただし，ログイン画面，ログアウト画面，および Reply-Message 表示画面では，Web 認証とのインタフェース用の記述が必要です。ログイン画面については「9.3.1　ログイン画面（login.html）」を，ログアウト画面については，「9.3.2　ログアウト画面（logout.html）」を，Reply-Message 表示画面については「9.3.3　Reply-Message 表示画面（loginProcess.html）【OP-OTP】」を参照してください。

また，「表 8-7　認証エラーメッセージとエラー発生理由対応表」に示した認証エラーメッセージも置き換えることができます。使用できるファイル名は次のとおりです。ファイルの作成方法については，「9.3.4　認証エラーメッセージファイル（webauth.msg）」を参照してください。

- 認証エラーメッセージ（ファイル名：webauth.msg）

さらに，Web ブラウザのお気に入りに表示するアイコンも入れ替えることができます。

- Web ブラウザのお気に入りに表示するアイコン（ファイル名：favicon.ico）

注意

入れ替え可能な画面および認証エラーメッセージのファイル名は，必ず上記に示したファイル名と一致させてください。

9.3.1 ログイン画面（login.html）

Web 認証にログインする際，ユーザ ID とパスワードの入力をクライアントに対し要求する画面です。

（1） 設定条件

ログイン画面の HTML ファイルを作成する際は，次の表に示す記述を必ず入れてください。

表 9-3　ログイン画面に必要な設定

記述内容	意味
<form name="Login" method="post" action="/cgi-bin/Login.cgi"></form>	ログイン操作を Web 認証に指示するための記述です。この記述は変更しないでください。

記述内容	意味
<input type="text" name="uid" size="40" maxlength="32" autocomplete="OFF" />	ユーザ ID を指定するための記述です。size と maxlength 以外の記述は変更しないでください。上記 <form></form> の内部に設定してください。また，maxlength は必ず 6 以上の数字を設定してください。
<input type="password" name="pwd" size="40" maxlength="32" autocomplete="OFF" />	パスワードを指定するための記述です。size と maxlength 以外の記述は変更しないでください。上記 <form></form> の内部に設定してください。また，maxlength は必ず 6 以上の数字を設定してください。
<input type="submit" value="Login" />	Web 認証にログイン要求を行うために記述です。この記述は変更しないでください。上記 <form></form> の内部に設定してください。

注意

login.html ファイルに，ほかのファイルを関連付ける場合は，関連付けするファイル名の先頭に ” / ” （スラッシュ）を記述してください。

（例） < img src="/image_file.gif" >

(2) 設定例

ログイン画面（login.html）のソース例を次の図に示します。

図 9-24 ログイン画面（login.html）のソース例

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title> </title>
</head>
<body>
<!-- ===== Body ===== -->
<center>
<br />
<table width="100%">
<tr><td align="center" bgcolor="#2b1872">
<font color="#ffffff"><b>LOGIN</b></font>
</td></tr></table>
<br />
Please enter your ID and password.<br />
<br />

<form name="Login" method="post" action="/cgi-bin/Login.cgi">
```

ログイン操作をWeb認証に指示するための記述

```
 <table><tr>
  <td>user ID</td>
  <td>

<input type="text" name="uid" size="40" maxlength="32" autocomplete="OFF" />
```

ユーザID指定のための記述

```
 </td>
 </tr><tr>
  <td>password</td>
  <td>

<input type="password" name="pwd" size="40" maxlength="32"
autocomplete="OFF" />
```

パスワード指定のための記述

```
 </td></tr>
 </table>
 <br />
<input type="submit" value="Login" />
```

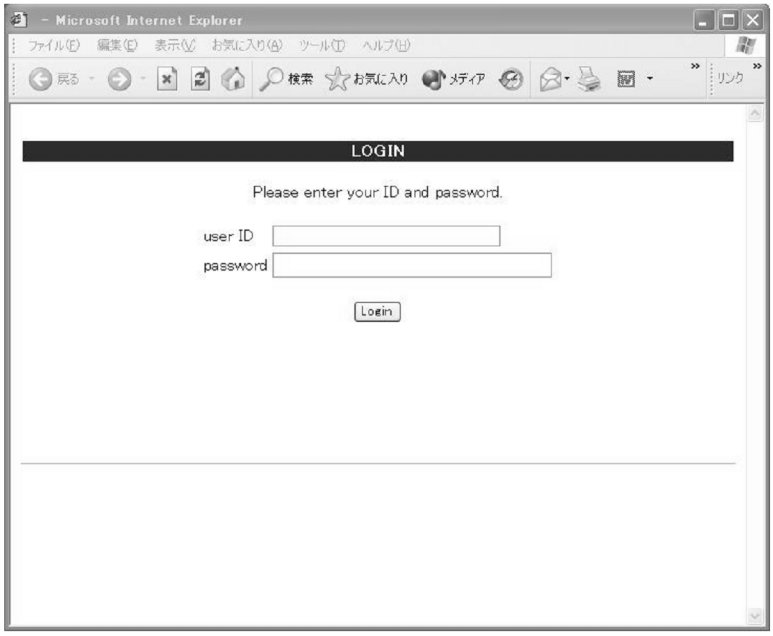
Web認証にログイン要求を行うための記述

```
 </form>
 <br /><br /><br /><br /><br />
 </center>
 <!-- ===== Footer ===== -->
 <hr>
 </body>
 </html>
```

(3) ログイン画面表示例

ログイン画面の表示例を次の図に示します。

図 9-25 ログイン画面の表示例



9.3.2 ログアウト画面（logout.html）

Web 認証機能でログインしているクライアントがログアウトを要求するための画面です。

(1) 設定条件

ログアウト画面の HTML ファイルを作成する際は，次の表に示す記述を必ず入れてください。

表 9-4 ログアウト画面に必要な設定

記述内容	意味
<form name="Logout" method="post" action="/cgi-bin/Logout.cgi"></form>	ログアウト操作を Web 認証に指示するための記述です。この記述は変更しないでください。
<input type="submit" value="Logout" />	Web 認証にログアウト要求を行うために記述です。この記述は変更しないでください。上記 <form></form> の内部に設定してください。

注意

logout.html ファイルに，ほかのファイルを関連付ける場合は，関連付けするファイル名の先頭に ” / ” （スラッシュ）を記述してください。

（例） < img src="/image_file.gif" >

(2) 設定例

ログアウト画面（logout.html）のソース例を次の図に示します。

図 9-26 ログアウト画面（logout.html）のソース例

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title> </title>
</head>
<body>
<!-- ===== Body ===== -->
<center>
<br />
<form name="Logout" method="post" action="/cgi-bin/Logout.cgi">
<table width="100%">
<tr><td align="center" bgcolor="#2b1872">
<font color="#ffffff"><b>LOGOUT</b></font>
</td></tr></table>
<br />
Please push the following button.<br />
<br />
<input type="submit" value="Logout" />
</form>
<br /><br /><br /><br /><br /><br />
</center>
<!-- ===== Footer ===== -->
<hr>
</body>
</html>
```

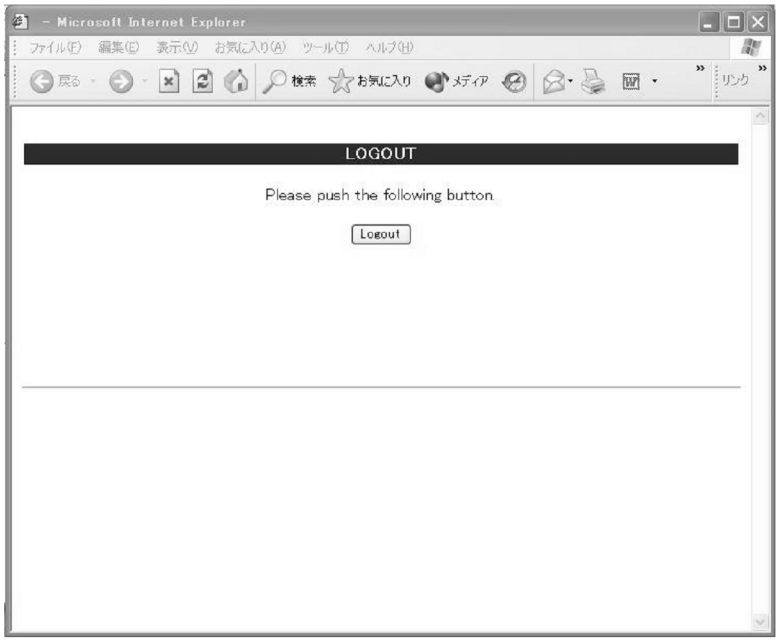
ログアウト操作をWeb認証に指示するための記述

Web認証にログアウト要求を行うための記述

(3) ログアウト画面表示例

ログアウト画面の表示例を次の図に示します。

図 9-27 ログアウト画面の表示例



9.3.3 Reply-Message 表示画面（loginProcess.html）【OP-OTP】

ワンタイムパスワード認証で使用する認証サーバから送られてくるメッセージを表示する画面です。

（1） 設定条件

Reply-Message 表示画面の HTML ファイルを作成する際は，次の表に示す記述を必ず入れてください。

表 9-5 Reply-Message 表示画面に必要な設定

記述内容	意味
<tbody> <tr> <td align="left" nowrap="nowrap"><!-- Reply_Message --></td> </tr> </tbody>	認証サーバから送られてくるメッセージを表示するための記述です。この記述は変更しないでください。
<form name="Process" method="post" action="/cgi-bin/Process.cgi">	Reply-Message 表示に対する操作を Web 認証に指示するための記述です。この記述は変更しないでください。
<input name="scode" type="hidden" value="<!-- Session_Code -->">	この記述は変更しないでください。
<input name="pcode" size="40" maxlength="32" autocomplete="OFF" type="password">	メッセージに対するデータを指定するための記述です。 size と maxlength 以外の記述は変更しないでください。 <form></form> の内部に設定してください。また， maxlength は必ず 6 以上の数字を設定してください。
<input value="Enter" type="submit">	Web 認証に要求を行うための記述です。この記述は変更しないでください。<form></form> の内部に設定してください。

注意

loginProcess.html ファイルに，ほかのファイルを関連付ける場合は，関連付けするファイル名の先頭に ”/”（スラッシュ）を記述してください。

（例） < img src="/image_file.gif" >

（2） 設定例

Reply-Message 表示画面（loginProcess.html）のソース例を次の図に示します。

図 9-28 Reply-Message 表示画面（loginProcess.html）のソース例

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">

<head>
 <meta http-equiv="Pragma" content="no-cache">
 <meta http-equiv="Cache-Control" content="no-cache">
 <meta http-equiv="Expires" content="Thu, 01 Dec 1994 16:00:00 GMT">
 <title> </title>
</head>

<body oncontextmenu="return false;">
<!-- ===== Body ===== -->
<center>
<br>
<table width="100%">
 <tbody>
 <tr>
  <td align="center" bgColor="#2b1872">
  <font color="#ffffff"><b>Reply Message</b></font></td>
 </tr>
 </tbody>
</table>
<br>                                                    メッセージを表示するための記述
<table align="center" border="0">
 <tbody>
 <tr>
  <td align="left" nowrap="nowrap"><!-- Reply_Message --></td>
 </tr>
 </tbody>
</table>
<br>                                                    Web認証に指示するための記述

<form name="Process" method="post" action="/cgi-bin/Process.cgi">
<input name="scode" type="hidden" value="<!-- Session_Code -->">
<table align="center" border="0">
 <tbody>                                                この行は変更しないでください
 <tr>
  <td align="left"><input name="pcode" size="40" maxlength="32"
autocomplete="OFF" type="password"></td>
  <td align="left"><input value="Enter" type="submit"></td>
 </tr>
 </tbody>                                                メッセージに対するデータ入力指定のための記述
</table>
</form>          Web認証に要求を行うための記述
<br>
<br>
<br>
<br>
<br>
<br>
</center>
<!-- ===== Footer ===== -->
<hr>
<div align="right"></div>
</body>
</html>
```

(3) Reply-Message 表示画面表示例

Reply-Message 表示画面の表示例を次の図に示します。

図 9-29 Reply-Message 表示画面の表示例

9.3.4 認証エラーメッセージファイル（webauth.msg）

認証エラーメッセージファイル（webauth.msg）は，Web 認証ログインまたは Web 認証ログアウトの失敗時に応答画面で表示するメッセージ群を格納したファイルです。

デフォルト設定の認証エラーメッセージを入れ替える際は，次の表に示す 9 行のメッセージを格納した認証エラーメッセージファイルを作成してください。

表 9-6 認証エラーメッセージファイルの各行の内容

行番号	内容
1 行目	ログイン時，ユーザ ID またはパスワード記述を誤った場合，もしくは Web 認証 DB による認証エラーとなった場合に出力するメッセージ。 ［デフォルトメッセージ］ “ User ID or password is wrong. Please enter correct user ID and password. ”
2 行目	Radius による認証エラーとなった場合に出力するメッセージ。 ［デフォルトメッセージ］ “ RADIUS: Authentication reject. ”
3 行目	コンフィグレーション上，Radius 認証の設定となっているが，Radius サーバと本装置との接続が確立していない場合に出力するメッセージ。 ［デフォルトメッセージ］ “ RADIUS: No authentication response. ”
4 行目	本装置のコンフィグレーションの設定誤り，または他機能との競合のためにログインできない場合に出力するメッセージ。 ［デフォルトメッセージ］ “ You cannot login by this machine. ”
5 行目	プログラムの軽度の障害が発生した場合に出力するメッセージ。 ［デフォルトメッセージ］ “ Sorry, you cannot login just now. Please try again after a while. ”
6 行目	プログラムの中度の障害が発生した場合に出力するメッセージ。 ［デフォルトメッセージ］ “ The system error occurred. Please contact the system administrator. ”
7 行目	プログラムの重度の障害が発生した場合に出力するメッセージ。 ［デフォルトメッセージ］ “ A fatal error occurred. Please inform the system administrator. ”

行番号	内容
8 行目	ログアウト処理で CPU 高負荷などによって，ログアウトが失敗した場合に出力するメッセージ。 ［デフォルトメッセージ］ “ Sorry, you cannot logout just now. Please try again after a while. ”
9 行目	ログインしていないユーザがログアウトした場合に出力するメッセージ。 ［デフォルトメッセージ］ “ The client PC is not authenticated. ”

(1) 設定条件

- 改行だけの行があった場合は，デフォルトのエラーメッセージを表示します。
- ファイル保存時は，改行コードを ” CR+LF ” または ” LF ” のどちらかで保存してください。
- 1 行に書き込めるメッセージ長は，半角 512 文字（全角 256 文字）までです。ここで示している文字数には html タグ，改行タグ ”
 ” も含みます。なお，半角 512 文字を超えた文字については無視します。
- 認証エラーメッセージファイルが 10 行以上あった場合は，10 行目以降の内容は無視します。

(2) 認証エラーメッセージファイル作成のポイント

- 認証エラーメッセージファイル上に記述したテキストは，そのまま HTML テキストとして使用します。したがって，認証エラーメッセージ上に HTML のタグを記述すると，そのタグの動作を行います。
- 1 メッセージは 1 行で記述する必要があるため，エラーメッセージの表示イメージに改行を入れたい場合は，改行したい個所に HTML の改行タグ ”
 ” を挿入してください。

(3) 設定例

認証エラーメッセージファイル（webauth.msg）のソース例を次の図に示します。

図 9-30 認証エラーメッセージファイル（webauth.msg）のソース例

```
ユーザID又はパスワードが不正です
パスワードが不正です
認証サーバが見つかりません<BR>システム管理者に問い合わせてください。
システムの設定に誤りがあります<BR>システム管理者に問い合わせてください。
システム障害発生（minor）<BR>しばらくしてから再度ログインをしてください。
システム障害発生（major）<BR>システム管理者に問い合わせてください。
システム障害発生（critical）<BR>システム管理者に問い合わせてください。
システムが高負荷状態です<BR>しばらくしてからログアウトしてください。
ログインしていません
```

(4) 表示例

上記の認証エラーメッセージファイルを使用し，パスワード長不正により，ログインに失敗したときのログイン失敗画面の表示例を次の図に示します。

図 9-31 ログイン失敗画面の表示例（パスワード長不正）

9.3.5 Web 認証固有タグ

Web 認証画面の HTML ファイルに Web 認証固有タグを書き込むことで，認証画面上にログイン時刻やエラーメッセージを表示できます。

設定可能な画面と Web 認証固有タグの組み合わせを次の表に示します。

表 9-7 特殊タグ一覧

タグ表記	画面に表示する内容	ログイン画面	ログアウト画面	ログイン成功画面	ログイン失敗画面	ログアウト完了画面	ログアウト失敗画面	Reply-Message 表示画面
<!-- Login_Time -->	ログイン時刻※1	－	－	○	－	－	－	－
<!-- Logout_Time -->	ログアウト時刻※2	－	－	○	－	○	－	－
<!-- After_Vlan -->	認証後 VLAN ID※3	－	－	○	－	－	－	－
<!-- Error_Message -->	エラーメッセージ※4	－	－	－	○	－	○	－
<!-- Redirect_URL -->	なし	－	－	_※5	－	－	－	－
<!-- Session_Code -->	なし	－	－	－	－	－	－	_※6
<!-- Reply_Message -->	RADIUS サーバから受信した Access-Challenge の Reply-Message	－	－	－	－	－	－	○

（凡例）○：画面上に表示する　－：画面上空欄となる
注※1　ログインが成功した時刻。

注※ 2　表示画面によって意味が異なります。
　　ログイン成功画面：自動ログアウトする時刻。
　　ログアウト完了画面：ログアウト動作が完了した時刻。
注※ 3　ログイン成功後，ユーザが通信を行う VLAN ID。
注※ 4　ログインまたはログアウトが失敗した場合のエラー要因。
注※ 5　画面上に表示しませんが，認証成功後のジャンプ先 URL を保持します。
注※ 6　画面上に表示しませんが，ユーザ ID と State 値を保持します。

設定例については，「9.3.6　その他の画面サンプル」を参照してください。

9.3.6　その他の画面サンプル

Web 認証画面（loginOK.html，logoutOK.html，loginNG.html，logoutNG.html）のサンプルソースを示します。

（1）ログイン成功画面（loginOK.html）

ログイン成功画面のソース例および表示例を次の図に示します。

図 9-32　ログイン成功画面のソース例（loginOK.html）

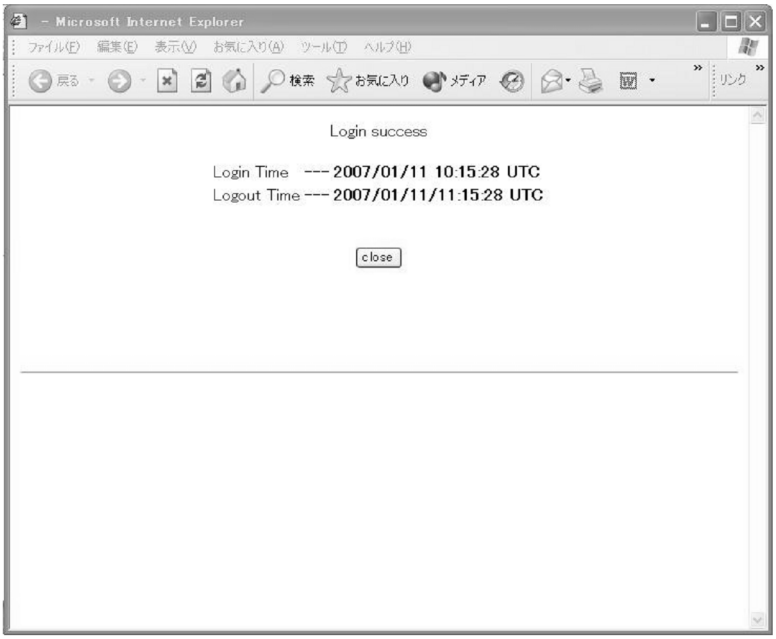
```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title> </title>
</head>
<body oncontextmenu=¥"return false;¥">
<!-- ===== Body ===== -->
<center>
Login success
<br /><br />
<Table Border="0">
<Tr>
<Td Align="left">
Login Time
</Td>
<Td Align="left">
 ---
</Td>
<Td Align="left">
<b><!-- Login_Time --></b>                    ログイン時刻表示タグ
</Td>
</Tr>
<Tr>
<Td Align="left">
Logout Time
</Td>
<Td Align="left">
 ---
</Td>
<Td Align="left">
<b><!-- Logout_Time --></b>                   ログアウト時刻表示タグ
</Td>
</Tr>
</Table>
<b><!-- Redirect_URL --></b>                  認証成功後のジャンプ先URLタグ
<br /><br />

<form>
<input type="button" value="close" onClick="window.close()" />
</form>
<br /><br />
</center>
<br /><br />
<!-- ===== Footer ===== -->
<hr>
</body>
</html>
```

注意

loginOK.html ファイルに，ほかのファイルを関連付ける場合は，関連付けするファイル名の先頭に ”/ ”（スラッシュ）を記述してください。

（例）＜ img src="/image_file.gif" ＞

図 9-33 ログイン成功画面の表示例



(2) ログアウト完了画面（logoutOK.html）

ログアウト完了画面のソース例および表示例を次の図に示します。

図 9-34 ログアウト完了画面のソース例（logoutOK.html）

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title> </title>
</head>
<body oncontextmenu=¥"return false;¥">
<!-- ===== Body ===== -->
<center>
Logout success
<br /><br />
Logout Time --- <b><!-- Logout_Time --></b>
<br /><br /><br />
<form>
<input type="button" value="close" onClick="window.close()" />
</form>
<br /><br />
</center>
<!-- ===== Footer ===== -->
<hr>
</body>
</html>
```

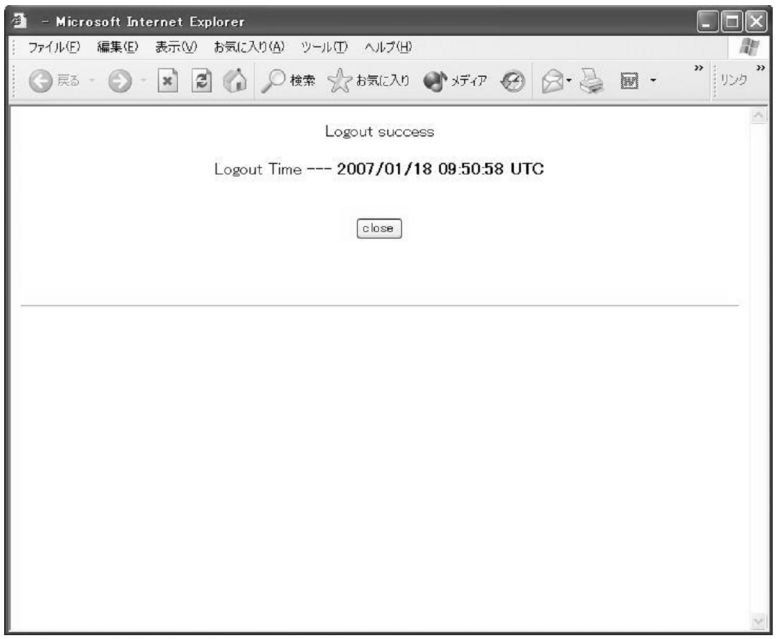
ログアウト時刻表示タグ

注意

logoutOK.html ファイルに，ほかのファイルを関連付ける場合は，関連付けするファイル名の先頭に ”/”（スラッシュ）を記述してください。

（例） ＜img src="/image_file.gif" ＞

図 9-35 ログアウト完了画面の表示例



(3) ログイン／ログアウト失敗画面（loginNG.html / logoutNG.html）

ログイン／ログアウト失敗画面のソース例および表示例を次の図に示します。

図 9-36 ログイン／ログアウト失敗画面のソース例（loginNG.html / logoutNG.html）

```
<?xml version="1.0" encoding="euc-jp"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<title> </title>
</head>
<body oncontextmenu=¥"return false;¥">
<!-- ===== Body ===== -->
<center>                                    エラーメッセージ表示タグ
<br>                                        ┌──────────────┐
<i style="color:red"><b><!-- Error_Message --></b></i>
<br /><br /><br /><br />
<form>
<input type="button" value="back" onClick="history.back()" />
<input type="button" value="close" onClick="window.close()" />
</form>
<br />
</center>
<!-- ===== Footer ===== -->
<hr>
</body>
</html>
```

注意

loginNG.html，logoutNG.html ファイルに，ほかのファイルを関連付ける場合は，関連付けするファイル名の先頭に ”/”（スラッシュ）を記述してください。

（例） < img src="/image_file.gif" >

図 9-37　ログイン／ログアウト失敗画面の表示例

10 MAC 認証の解説

MAC 認証は，受信したフレームの送信元 MAC アドレスを認証し，VLAN へのアクセス制御を行う機能です。この章では MAC 認証について解説します。

10.1 概要

ユーザ ID，パスワードを入力できる PC のような機器では IEEE802.1X や Web 認証を利用できますが，MAC 認証はユーザ ID，パスワードを入力できないプリンタなどの機器でも認証を行うための機能です。

指定されたポートに受信するフレームの送信元 MAC アドレスで認証し，認証された MAC アドレスを持つフレームだけが通信を許可されます。

なお，DHCP snooping が設定された場合，MAC 認証の対象となる端末から送信された ARP パケットと DHCP パケットは MAC 認証よりも先に DHCP snooping の対象となるため，DHCP snooping で許可されたパケットだけが MAC 認証の対象となります。

(1) 認証モード

本装置は次に示す認証モードをサポートしています。

- 固定 VLAN モード
  認証が成功した端末の MAC アドレスを MAC アドレステーブルに登録して，VLAN へ通信できるようにします。
- ダイナミック VLAN モード
  認証が成功したあと，MAC アドレスを MAC VLAN に登録して，認証前のネットワークと認証後のネットワークを分離します。

ダイナミック VLAN モードの記述で，認証前の端末が所属する VLAN を認証前 VLAN と呼びます。また，認証後の VLAN を認証後 VLAN と呼びます。

(2) 認証方式

本装置は固定 VLAN モード，ダイナミック VLAN モードのどちらの認証モードでも，次に示すローカル認証方式または RADIUS 認証方式のどちらかの方式を選択できます。

- ローカル認証方式
  本装置に内蔵した認証用 DB（**内蔵 MAC 認証 DB** と呼びます）に MAC アドレスを登録しておき，受信したフレームの MAC アドレスとの一致を確認して認証する方式です。ネットワーク内に RADIUS サーバを置かない小規模ネットワークに適しています。
- RADIUS 認証方式
  ネットワーク内に設置した RADIUS サーバを用いて認証する方式です。比較的規模の大きなネットワークに適しています。

10.2 システム構成例

ここでは，固定 VLAN モードおよびダイナミック VLAN モードの各認証モードについて，ローカル認証方式および RADIUS 認証方式の場合のシステム構成を示します。

10.2.1 固定 VLAN モード

固定 VLAN モードでは，認証対象端末が認証前のときは，MAC アドレステーブルに登録されず，接続された VLAN 内へ通信できない状態です。認証が成功すると，端末の MAC アドレスを MAC アドレステーブルに登録し，VLAN 内へ通信できるようになります。

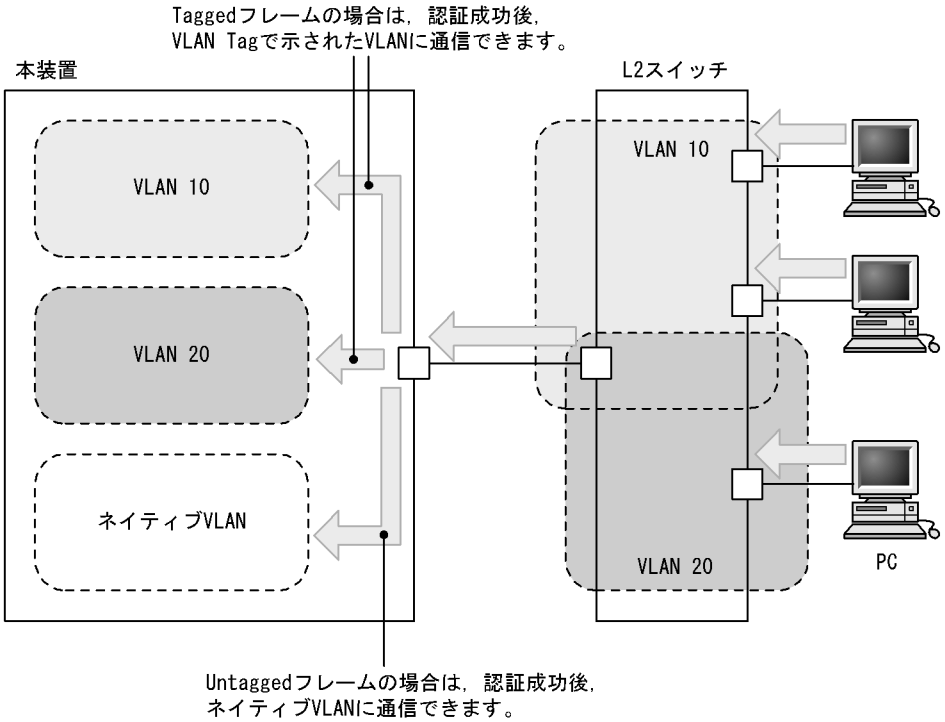
本装置では，認証ポートとして次のポートを設定できます。

- アクセスポート
- トランクポート

トランクポートに入ってきた Tagged フレームおよび Untagged フレームの扱いを次に示します。

- 認証時のフレームが Tagged フレームの場合，認証成功後，VLAN Tag で示された VLAN に通信できます。
- 認証時のフレームが Untagged フレームの場合，認証成功後，ネイティブ VLAN に通信できます。

図 10-1 Tagged フレームおよび Untagged フレームの扱い

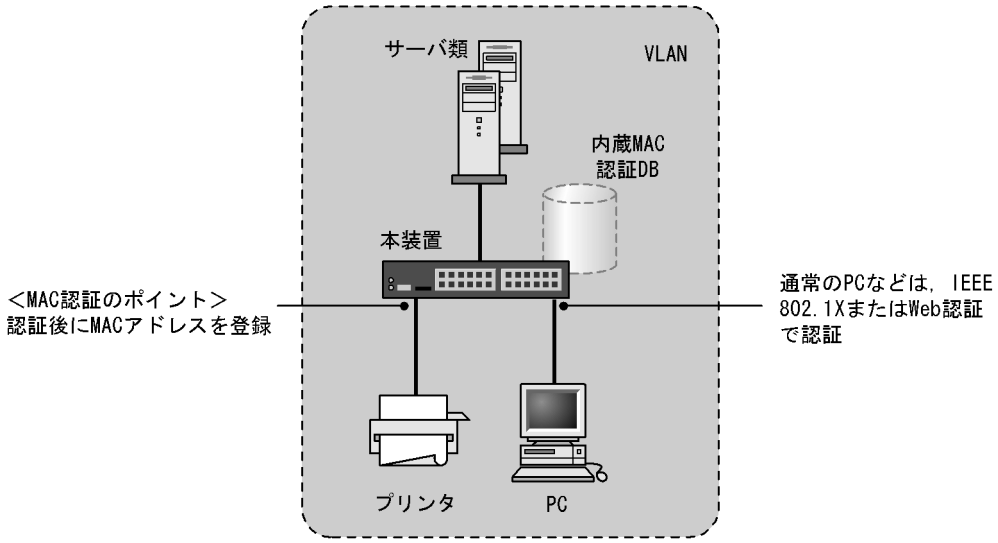


また，認証前 VLAN 内で通信したい場合は，認証専用 IPv4 アクセスリストで通信に必要なフィルタ条件を設定する必要があります。

(1) ローカル認証方式

ローカル認証方式は，MAC 認証の対象となるポートで受信したフレームの送信元 MAC アドレスと，内蔵 MAC 認証 DB に登録されている MAC アドレスとを照合し，一致していれば認証成功として通信を許可する方式です。

図 10-2 固定 VLAN モードのローカル認証方式の構成



なお，ローカル認証方式には，MAC アドレスだけで照合する方法と，MAC アドレスと VLAN ID との組み合わせで照合する方法があります。これらの方法は，コンフィグレーションコマンド mac-authentication vlan-check で選択できます。

MAC アドレスと VLAN ID による照合時の設定条件を次の表に示します。

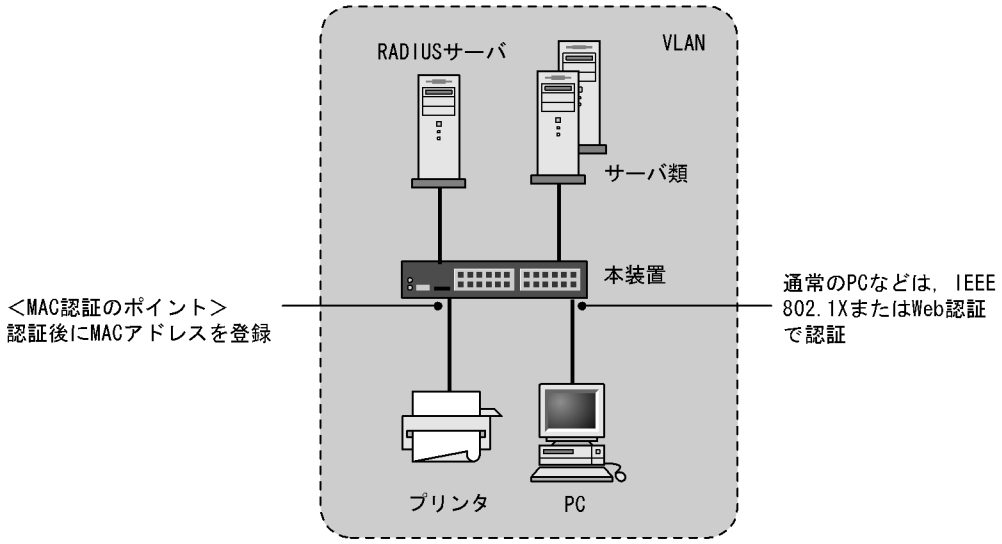
表 10-1 固定 VLAN モードのローカル認証方式の VLAN ID 照合

コンフィグレーションコマンド設定	内蔵 MAC 認証 DB の VLAN ID 設定	
	有り	無し
有り	MAC アドレスと VLAN ID で照合します。	MAC アドレスだけで照合します。
無し	MAC アドレスだけで照合します。	MAC アドレスだけで照合します。

(2) RADIUS 認証方式

RADIUS 認証方式は，MAC 認証の対象となるポートで受信したフレームの送信元 MAC アドレスと，RADIUS サーバに登録されている MAC アドレスとを照合し，一致していれば認証成功として通信を許可する方式です。

図 10-3 固定 VLAN モードの RADIUS 認証方式の構成



なお，RADIUS 認証方式には，MAC アドレスだけで照合する方法と，MAC アドレスと VLAN ID との組み合わせで照合する方法があります。これらの方法は，コンフィグレーションコマンド mac-authentication vlan-check で選択できます。

MAC アドレスと VLAN ID による照合時の設定条件を次の表に示します。

表 10-2 固定 VLAN モードの RADIUS 認証方式の VLAN ID 照合

コンフィグレーション コマンド設定	動作
有り	MAC アドレスと VLAN ID で照合します。
無し	MAC アドレスだけで照合します。

また，RADIUS への問い合わせに用いるパスワードは，コンフィグレーションコマンド mac-authentication password で設定できます。なお，コンフィグレーションコマンド mac-authentication password が設定されていない場合は，認証を行う MAC アドレスをパスワードとして用います。

10.2.2 ダイナミック VLAN モード

ダイナミック VLAN モードでは，認証前 VLAN に収容されていた認証対象端末を，認証成功後，内蔵 MAC 認証 DB または RADIUS に登録されている VLAN ID を使用して，MAC VLAN と MAC アドレステーブルに登録して認証後 VLAN への通信を許可します。このため，次に示す設定が必要になります。

- MAC VLAN が設定されている MAC ポートを認証ポートとして設定

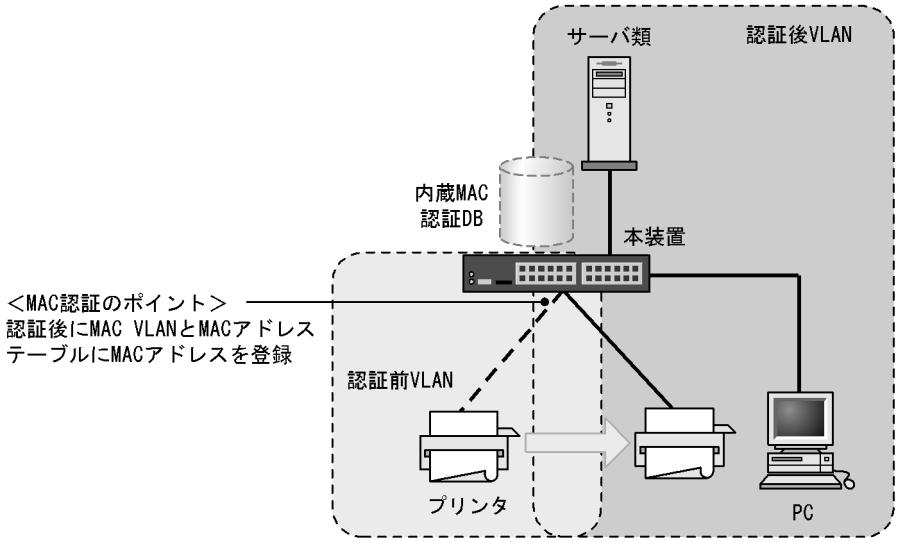
また，認証前 VLAN 内で通信したい場合は，認証専用 IPv4 アクセスリストで通信に必要なフィルタ条件を設定する必要があります。

(1) ローカル認証方式

ローカル認証方式は，MAC 認証の対象となるポートで受信したフレームの送信元 MAC アドレスと，内蔵 MAC 認証 DB に登録されている MAC アドレスとを照合し，一致していれば認証成功として内蔵 MAC 認

証 DB に登録されている VLAN ID を使用して，MAC VLAN と MAC アドレステーブルに登録し，認証後 VLAN への通信を許可する方式です。

図 10-4 ダイナミック VLAN モードのローカル認証方式の構成

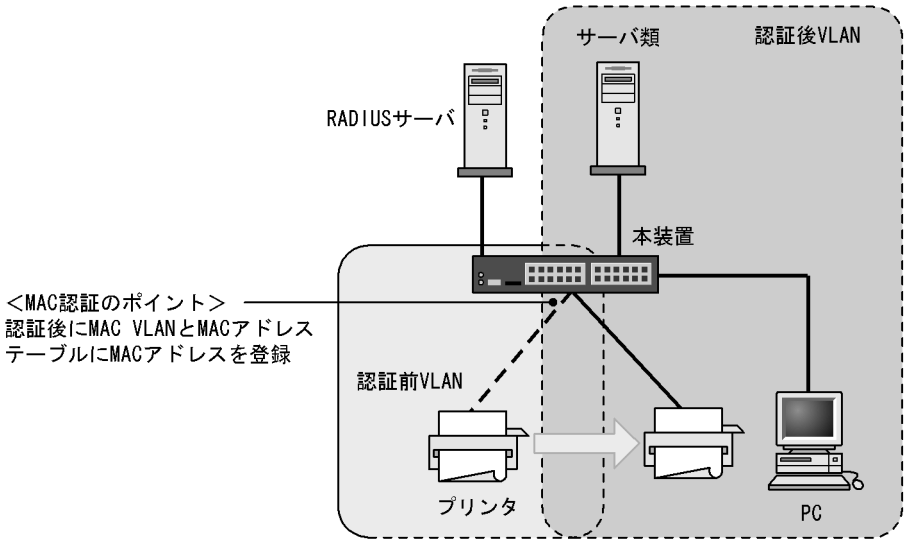


(2) RADIUS 認証方式

RADIUS 認証方式は，MAC 認証の対象となるポートで受信したフレームの送信元 MAC アドレスと，RADIUS サーバに登録されている MAC アドレスとを照合し，一致していれば RADIUS に登録されている VLAN ID を使用して，MAC VLAN と MAC アドレステーブルに登録して認証後 VLAN への通信を許可する方式です。

また，RADIUS への問い合わせに使用するパスワードは，コンフィグレーションコマンド mac-authentication password で設定できます。コンフィグレーションコマンド mac-authentication password が設定されていない場合は，認証する MAC アドレスをパスワードとして使用します。

図 10-5　ダイナミック VLAN モードの RADIUS 認証方式の構成



10.2.3　MAC ポートに dot1q 設定時の動作

MAC ポートに dot1q が設定された場合の動作については,「5.3　レイヤ 2 認証共通の機能」を参照してください。

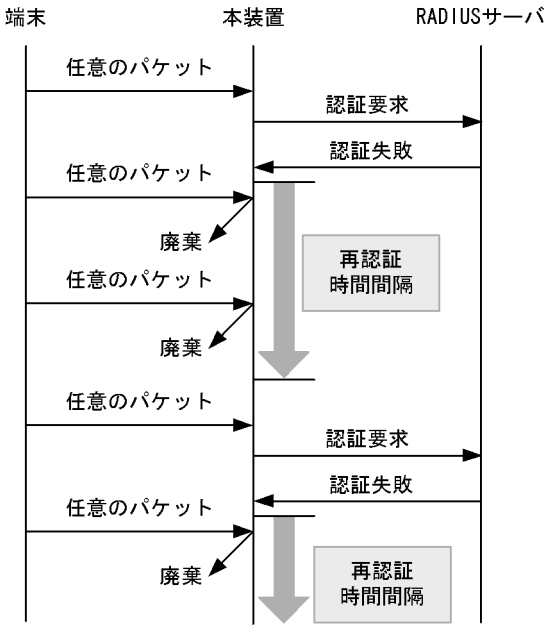
10.3 認証機能

10.3.1 認証失敗後の動作

端末の認証に失敗した場合，一定時間（再認証時間間隔と呼びます）は MAC 認証での認証をしません。再認証時間間隔経過後，改めて認証処理を行います。

なお，コンフィグレーションコマンド mac-authentication auth-interval-timer によって再認証時間間隔を設定できます。設定された再認証時間間隔を超過してから 1 分以内に改めて認証処理を行います。

図 10-6 認証失敗後の動作シーケンス



10.3.2 強制認証

MAC 認証の強制認証動作については，「5.3 レイヤ 2 認証共通の機能」を参照してください。

10.3.3 認証解除方式

端末の認証解除方式を次の表に示します。

表 10-3 認証モードごとの認証解除方式

認証解除方式	固定 VLAN モード	ダイナミック VLAN モード
最大接続時間超過時の認証解除	○	○
運用コマンドによる認証解除	○	○
認証端末接続ポートのリンクダウンによる認証解除	○	－
認証済み端末の MAC アドレステーブルエージングによる認証解除	○	○
VLAN 設定変更による認証解除	○	○
認証方式の切り替えによる認証解除	○	○

認証解除方式	固定 VLAN モード	ダイナミック VLAN モード
認証モードの切り替えによる認証解除	○	○
MAC 認証の停止による認証解除	○	○
動的に登録された VLAN の削除によるログアウト	－	○

（凡例） ○：サポート －：該当なし

(1) 最大接続時間超過時の認証解除

コンフィグレーションコマンド mac-authentication max-timer で設定された最大接続時間を超えた場合に，強制的に認証状態を解除します。この際に設定された最大接続時間を経過してから 1 分以内で認証解除が行われます。

なお，コンフィグレーションコマンド mac-authentication max-timer で最大接続時間を短縮したり，延長したりした場合，現在認証中の端末には適用されず，次回認証時から設定が有効となります。

(2) 運用コマンドによる認証解除

運用コマンド clear mac-authentication auth-state で MAC アドレス単位に，強制的に認証解除ができます。なお，同一 MAC アドレスで複数の VLAN ID に認証を行っている場合は，同じ MAC アドレスを持つ認証をすべて解除します。

(3) 認証端末接続ポートのリンクダウンによる認証解除

認証済み端末が接続しているポートのリンクダウンを検出した際に，該当するポートに接続された端末の認証を解除します。

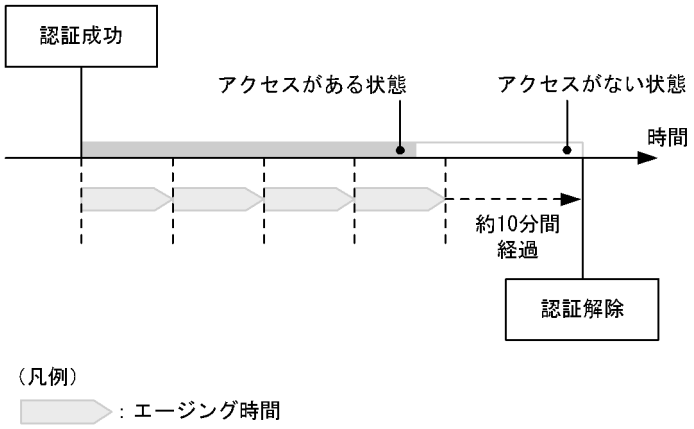
(4) 認証済み端末の MAC アドレステーブルエージングによる認証解除

認証済み端末に対し，MAC アドレステーブルを周期的に監視し，端末からのアクセスがあるかをチェックしています。該当する端末からのアクセスがない状態が続いた場合に，強制的に MAC 認証の認証状態を解除し，認証前の VLAN ID に収容を変更します。ただし，回線の瞬断などの影響で認証が解除されてしまうことを防ぐために，MAC アドレステーブルのエージング時間経過後約 10 分間，該当する MAC アドレスを持つ端末からのアクセスがない状態が続いた場合に，認証状態を解除します。

MAC アドレステーブルのエージング時間と，MAC アドレステーブルエージングによるログアウトの関係を次の図に示します。

なお，MAC アドレステーブルのエージング時間はデフォルト値を使用するか，またはデフォルト値より大きな値を設定してください。

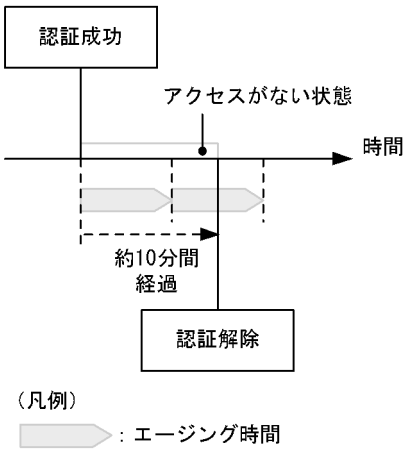
図 10-7　認証済み端末の MAC アドレステーブルエージングによるログアウト



また，認証成功直後約 10 分間に端末からのアクセスがないと，エージング時間の値に関係なく，強制的に認証を解除します。

認証成功直後からアクセスがない場合のログアウトを次の図に示します。

図 10-8　認証成功直後からアクセスがない場合のログアウト



なお，この機能はコンフィグレーションコマンド no mac-authentication auto-logout で無効にできます（アクセスがない状態が続いた場合でも強制的にログアウトしない設定が可能）。

（5）VLAN 設定変更による認証解除

コンフィグレーションコマンドで認証端末が含まれる VLAN の設定を変更した場合，変更された VLAN に含まれる端末の認証を解除します。

［コンフィグレーションの変更内容］

- VLAN を削除した場合
- VLAN を停止（suspend）した場合

（6）認証方式の切り替えによる認証解除

認証方式が RADIUS 認証方式からローカル認証方式に切り替わった場合，またはローカル認証方式から RADIUS 認証方式に切り替わった場合，すべての端末の認証を解除します。

(7) 認証モードの切り替えによる認証解除

copy コマンドでコンフィグレーションを変更して，認証モードが切り替わる設定をした場合，すべての端末の認証を解除します。

(8) MAC 認証の停止による認証解除

コンフィグレーションコマンドで MAC 認証の定義が削除されて MAC 認証が停止した場合，すべての端末の認証を解除します。

(9) 動的に登録された VLAN の削除によるログアウト

動的に VLAN が作成された認証ポートにコンフィグレーションコマンド switchport mac vlan が設定された場合，該当ポートに動的に作成された VLAN ID は削除されて，VLAN に所属していた端末の認証を解除します。

10.3.4 認証数制限

装置単位およびポート単位に認証数の制限が設定できます。詳細は，「5.3 レイヤ 2 認証共通の機能」を参照してください。

10.3.5 認証済み端末のポート間移動

認証済み端末がポート間を移動した場合については，「5.3 レイヤ 2 認証共通の機能」を参照してください。

10.3.6 アカウント機能

認証結果は次のアカウント機能によって記録されます。

(1) アカウントログ

認証結果は，本装置の MAC 認証のアカウントログに記録されます。記録されたアカウントログは，運用コマンド show mac-authentication logging で表示できます。

出力される認証結果を次の表に示します。

表 10-4 出力される認証結果

事象	時刻	MAC アドレス	VLAN ID	ポート番号	メッセージ
認証成功	認証成功時刻	○	○	○	成功メッセージ
認証解除	認証解除時刻	○	○※	○※	解除メッセージ
認証失敗	認証失敗時刻	○	○※	○※	失敗要因メッセージ

（凡例）○：記録する
注※ メッセージによっては出力されない場合があります。

本装置の MAC 認証のアカウントログは，最大 2100 行まで記録できます。2100 行を超えた場合，古い順に記録が削除され，最新のアカウント情報が追加記録されていきます。

(2) RADIUS サーバのアカウント機能への記録

コンフィグレーションコマンド aaa accounting mac-authentication で，RADIUS サーバのアカウント機

能を使用できます。アカウント機能には次の情報が記録されます。

- 認証情報　　：認証成功時に次の情報が記録されます。
  サーバに記録された時刻，MAC アドレス，VLAN ID
- 認証解除情報　：認証解除時に次の情報が記録されます。
  サーバに記録された時刻，MAC アドレス，VLAN ID，認証成功から認証解除までの経過時間

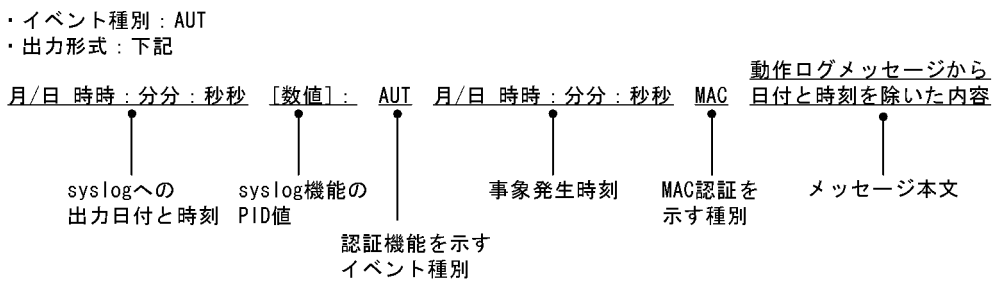
(3) RADIUS サーバへの認証情報記録

RADIUS 認証方式の場合は，RADIUS サーバが持っている機能によって，認証成功／認証失敗が記録されます。ただし，使用する RADIUS サーバによって記録される情報が異なることがありますので，詳細は RADIUS サーバの説明書を参照してください。

(4) syslog サーバへの動作ログ記録

MAC 認証の動作ログを syslog サーバに出力できます。また，動作ログは MAC 認証のアカウントログを含みます。syslog サーバへの出力形式を次の図に示します。

図 10-9　syslog サーバ出力形式



また，コンフィグレーションコマンド mac-authentication logging enable および logging event-kind aut によって，出力の開始および停止ができます。

10.4 内蔵 MAC 認証 DB および RADIUS サーバの準備

10.4.1 内蔵 MAC 認証 DB の準備

MAC 認証のローカル認証方式を使用するに当たって，事前に内蔵 MAC 認証 DB を作成する必要があります。また，本装置の内蔵 MAC 認証 DB はバックアップおよび復元できます。

(1) 内蔵 MAC 認証 DB の作成

運用コマンド set mac-authentication mac-address で MAC アドレスおよび VLAN ID を内蔵 MAC 認証 DB に登録します。運用コマンド remove mac-authentication mac-address で登録した MAC アドレスの削除もできます。

登録・変更された内容は，運用コマンド commit mac-authentication が実行された時点で，内蔵 MAC 認証 DB に反映されます。

なお，運用コマンド commit mac-authentication で内蔵 MAC 認証 DB への反映を行った場合，現在認証中の端末には適用されず，次回認証時から有効となります。

注意

内蔵 MAC 認証 DB をダイナミック VLAN モードで使用する場合は，登録時に次の点に注意する必要があります。

- MAC アドレス登録時に必ず VLAN ID を指定してください。VLAN ID が省略されている場合は，その MAC アドレスは認証エラーとなります。
- 同じ MAC アドレスを複数の VLAN ID で登録した場合，最も数字の小さい VLAN ID が VLAN 切り替えに使用されます。
- VLAN ID に 1 を指定しないでください。MAC VLAN で使用できない VLAN ID のために認証エラーとなります。

(2) 内蔵 MAC 認証 DB のバックアップ

運用コマンド store mac-authentication で，ローカル認証用に作成した内蔵 MAC 認証 DB のバックアップを取ることができます。

(3) 内蔵 MAC 認証 DB の復元

運用コマンド load mac-authentication で，ローカル認証用に作成したバックアップファイルから，内蔵 MAC 認証 DB の復元ができます。ただし，復元を実行すると，直前に運用コマンド set mac-authentication mac-address で登録・更新していた内容は廃棄されて，復元された内容に置き換わりますので，注意が必要です。

10.4.2 RADIUS サーバの準備

MAC 認証の RADIUS 認証方式を使用するに当たっては，事前に MAC アドレスとパスワードを RADIUS サーバに設定する必要があります。

また，本装置の MAC 認証機能が使用する RADIUS の属性を示します。

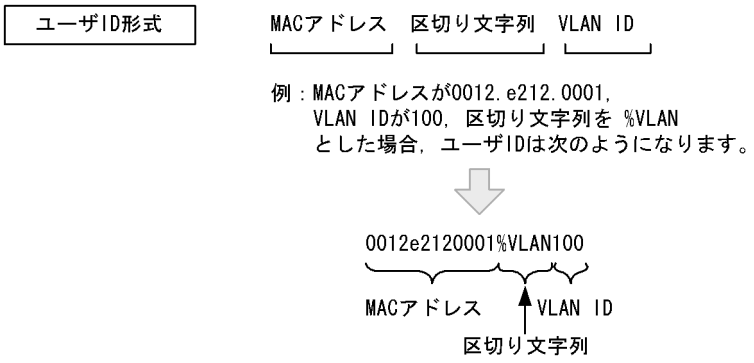
(1) ユーザ ID の登録

MAC アドレスの照合用として RADIUS のユーザ ID に MAC アドレスを登録します。MAC アドレスは

16 進文字列で半角英数字（英字は a ～ f の小文字）を用い，12 文字で指定します。

また，固定 VLAN モードで，RADIUS での照合時に MAC アドレスだけでなく VLAN ID も照合したい場合は，次に示す形式で MAC アドレスと VLAN ID を表す文字列とをつないだものをユーザ ID として登録してください。

図 10-10　MAC アドレス +VLAN ID 登録形式



(2) パスワードの登録

次のどちらかをパスワードとして設定します。

- ユーザ ID に登録した MAC アドレスと同一の MAC アドレス
- ユーザ ID に共通の文字列

(3) 認証後 VLAN の設定

ダイナミック VLAN モードで認証成功後に切り替える認証後 VLAN を次のように設定します。

1. Tunnel-Type に Virtual LANs（VLAN）を設定（値 13）します。
2. Tunnel-Medium-Type に 6 を設定します。
3. Tunnel-Private-Group-ID に VLAN ID を次の形式で設定します。

- 数字文字で設定
  例：VLAN ID が 2048 の場合，文字列で 2048 を設定
- 文字列 ” VLAN ” に続いて VLAN ID を数字文字で設定
  例：VLAN ID が 2048 の場合，VLAN2048 を設定
- コンフィグレーションコマンド name で設定した VLAN 名称を設定

なお，Tunnel-Type，Tunnel-Medium-Type，および Tunnel-Private-Group-ID の三つの属性がすべて設定されていない状態でダイナミック VLAN モードで使用した場合，認証後 VLAN としてネイティブ VLAN を適用します。

(4) MAC 認証機能が使用する RADIUS サーバの属性

認証方式として PAP を設定します。また，MAC 認証が使用する RADIUS の属性を次の表に示します。なお，RADIUS サーバの詳細な設定方法については，使用する RADIUS サーバの説明書を参照してください。

表 10-5 MAC 認証で使用する属性名（その 1 Access-Request）

属性名	Type 値	説明
User-Name	1	MAC アドレス，または「図 10-10 MAC アドレス +VLAN ID 登録形式」で生成した値を指定します。
User-Password	2	MAC アドレス，またはコンフィグレーションコマンドで設定されたパスワードを指定します。
NAS-IP-Address	4	ループバックインタフェースの IP アドレス指定時はループバックインタフェースの IP アドレスを格納し，指定されていなければ RADIUS サーバと通信するインタフェースの IP アドレスを格納します。
Service-Type	6	Framed(2) を設定します。
Calling-Station-Id	31	認証端末の MAC アドレス（小文字 ASCII, “ - ” 区切り）を指定します。 例：00-12-e2-01-23-45
NAS-Identifier	32	固定 VLAN モードでは，認証端末を収容している VLAN ID を数字文字列で指定します。 例：VLAN ID 100 の場合 100 ダイナミック VLAN モードでは，コンフィグレーションコマンド hostname で指定された装置名を指定します。
NAS-Port-Type	61	Virtual(5) を設定します
NAS-IPv6-Address	95	ループバックインタフェースの IPv6 アドレス指定時はループバックインタフェースの IPv6 アドレスを格納し，指定されていなければ RADIUS サーバと通信するインタフェースの IPv6 アドレスを格納します。ただし，IPv6 リンクローカルアドレスで通信する場合は，ループバックインタフェースの IPv6 アドレス設定の有無にかかわらず，送信インタフェースの IPv6 リンクローカルアドレスを格納します。

表 10-6 MAC 認証で使用する属性名（その 2 Access-Accept）

属性名	Type 値	説明
Service-Type	6	Framed(2) が返却される：MAC 認証ではチェックしません。
Reply-Message	18	（未使用）
Tunnel-Type	64	ダイナミック VLAN モード時に使用します。 VLAN を示す 13 であるかをチェックします。 固定 VLAN モード時は使用しません。
Tunnel-Medium-Type	65	ダイナミック VLAN モード時に使用します。 IEEE802.1X と同様の値 6 の Tunnel-Medium-Type であるかをチェックします。 固定 VLAN モード時は使用しません。
Tunnel-Private-Group-Id	81	ダイナミック VLAN モード時に使用します。 VLAN を表す数字文字列または “ VLANxx ” xx は VLAN ID を表します。 ただし，先頭の 1 オクテットの内容が 0x00 ～ 0x1f の場合は，Tag を表しているので，この場合は 2 オクテット目からの値が VLAN を表します。先頭の 1 オクテットの内容が 0x20 以上の場合は，先頭から VLAN を表します。 また，コンフィグレーションコマンド name で設定された VLAN 名称が指定された場合は，VLAN 名称に対応する VLAN ID を使用します。 固定 VLAN モード時は使用しません。

表 10-7 RADIUS Accounting で使用する属性名

属性名	Type 値	説明
User-Name	1	MAC アドレス，または「図 10-10 MAC アドレス +VLAN ID 登録形式」で生成した値を指定します。
NAS-IP-Address	4	NAS の IP アドレスを格納します。 ループバックインタフェースの IP アドレス設定時は，ループバックインタフェースの IP アドレスを格納します。なお，これ以外は，サーバと通信するインタフェースの IP アドレスを格納します。
Service-Type	6	Framed(2) を設定します。
Calling-Station-Id	31	端末の MAC アドレス（小文字 ASCII, “ - ” 区切り）を設定します。 例：00-12-e2-01-23-45
NAS-Identifier	32	固定 VLAN モードでは，認証端末を収容している VLAN ID を数字文字列で設定します。 例：VLAN ID 100 の場合 100 ダイナミック VLAN モードでは，コンフィグレーションコマンド hostname で指定された装置名を指定します。
Acct-Status-Type	40	認証成功時に Start(1)，認証解除時に Stop(2) を格納します。
Acct-Delay-Time	41	イベント発生時から送信するまでに要した時間（秒）を格納します。
Acct-Session-Id	44	プロセス ID を格納します。（認証成功，認証解除に関しては同じ値です）
Acct-Authentic	45	認証方式を示す RADIUS，Local のどちらかを格納します。
Acct-Session-Time	46	認証解除するまでの時間（秒）を格納します。
NAS-Port-Type	61	Virtual(5) を設定します。
NAS-IPv6-Address	95	NAS の IPv6 アドレスを格納します。 ループバックインタフェースの IPv6 アドレス設定時は，ループバックインタフェースの IPv6 アドレスを格納します。なお，これ以外は，サーバと通信するインタフェースの IPv6 アドレスを格納します。ただし，IPv6 リンクローカルアドレスで通信する場合は，ループバックインタフェースの IPv6 アドレス設定の有無にかかわらず，送信インタフェースの IPv6 リンクローカルアドレスを格納します。

10.5 MAC 認証使用時の注意事項

(1) 他機能との共存

他機能との共存については,「5.2 レイヤ 2 認証と他機能との共存について」を参照してください。

(2) MAC 認証プログラムが再起動した場合

MAC 認証プログラムが再起動した場合，認証中のすべての認証が解除されます。この場合，再起動後に再度認証を行ってください。

(3) MAC 認証と IP マルチキャストパケットフロー制御補助モードとの共存時の動作

MAC 認証と IP マルチキャストパケットフロー制御補助モードを同時に使用した場合，次に示すパケットでの認証はしません。

- 宛先アドレスが IPv4 マルチキャストアドレスのパケット
- 宛先アドレスの範囲が ff0::/12 以外の IPv6 マルチキャストパケット
- MLD パケット

11 MAC 認証の設定と運用

MAC 認証は，受信したフレームの送信元 MAC アドレスを認証し，VLAN へのアクセス制御を行う機能です。この章では MAC 認証のオペレーションについて説明します。

11.1 コンフィグレーション

11.1.1 コンフィグレーションコマンド一覧

MAC 認証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 11-1 コンフィグレーションコマンド一覧

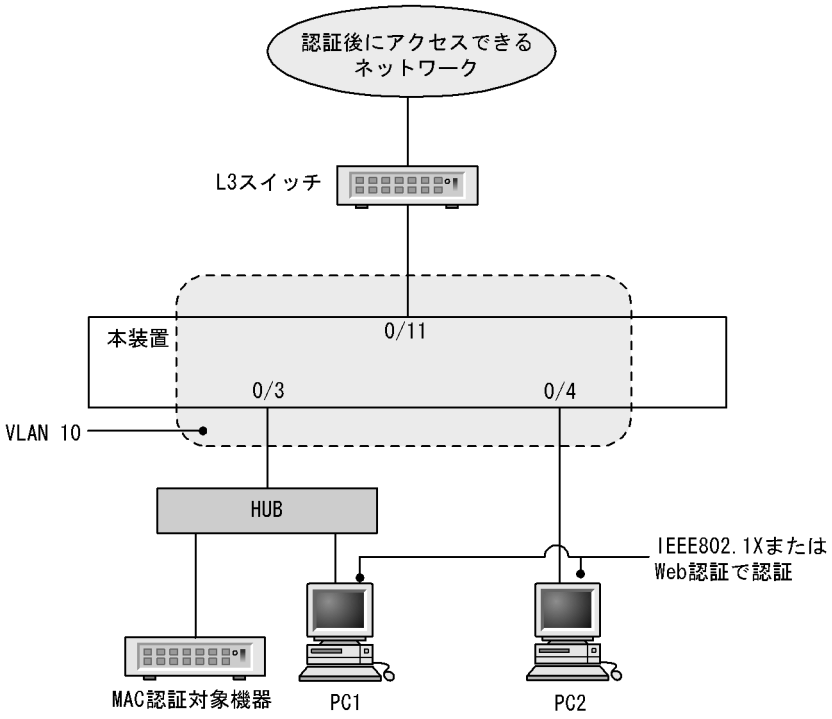
コマンド名	説明
aaa accounting mac-authentication default start-stop group radius	RADIUS Accounting を使用することを設定します。
aaa authentication mac-authentication default group radius	RADIUS 認証方式で認証することを設定します。
mac-authentication auth-interval-timer	認証失敗後，次の認証が行われるまでの再認証時間間隔を指定します。
mac-authentication auto-logout	端末からのアクセスがない状態が続いていることを検出して認証解除する動作を無効にします。
mac-authentication dot1q-vlan force-authorized	MAC ポートに switchport mac dot1q vlan 設定がある場合に，Tagged フレームを認証除外に設定します。
mac-authentication dynamic-vlan max-user	ダイナミック VLAN モードで認証できる MAC アドレス数を指定します。
mac-authentication logging enable	動作ログの syslog サーバへの出力を設定します。
mac-authentication max-timer	認証最大時間を指定します。
mac-authentication password	RADIUS サーバへの問い合わせ時に使用するパスワードを指定します。
mac-authentication port	MAC 認証を行うポートを設定します。
mac-authentication radius-server host	MAC 認証専用に RADIUS サーバの IP アドレスなどを指定します。
mac-authentication static-vlan max-user	固定 VLAN モードで認証できる MAC アドレス数を指定します。
mac-authentication system-auth-control	MAC 認証デーモンを起動します。
mac-authentication vlan-check	認証時に MAC アドレスに加え，VLAN ID も照合することを設定します。

11.1.2 固定 VLAN モードのコンフィグレーション

(1) ローカル認証方式の基本的な設定

固定 VLAN モードで，ローカル認証方式を使用する上での基本的な設定を次の図に示します。

図 11-1 固定 VLAN モードのローカル認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

MAC 認証で使用するポートを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/3**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# mac-authentication port
   (config-if)# exit
   認証を行う端末が接続されているポートに MAC 認証を設定します。

(b) MAC 認証の設定

[設定のポイント]

MAC 認証のコンフィグレーションコマンドを設定して MAC 認証を有効にします。

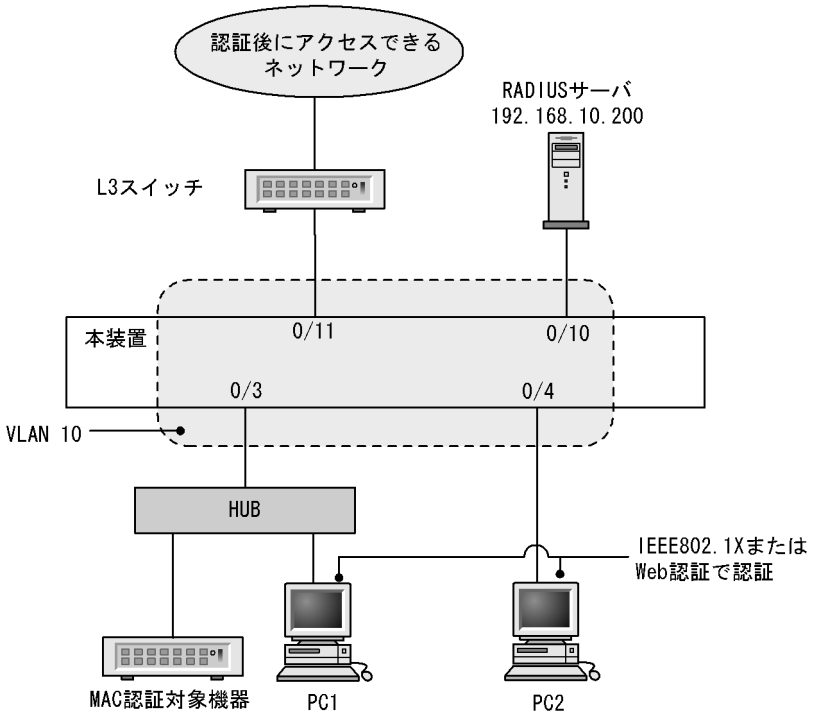
[コマンドによる設定]

1. **(config)# mac-authentication system-auth-control**
   MAC 認証を起動します。

(2) RADIUS 認証方式の基本的な設定

固定 VLAN モードで，RADIUS 認証方式を使用する上での基本的な設定を次の図に示します。

図 11-2 固定 VLAN モードの RADIUS 認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

MAC 認証で使用するポートを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/3**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# mac-authentication port
   (config-if)# exit
   認証を行う端末が接続されているポートに MAC 認証を設定します。

(b) MAC 認証の設定

[設定のポイント]

MAC 認証のコンフィグレーションコマンドを設定して MAC 認証を有効にします。

[コマンドによる設定]

1. **(config)# aaa authentication mac-authentication default group radius**
   (config)# mac-authentication radius-server host 192.168.10.200 key "macauth"
   認証を RADIUS サーバでするために，IP アドレスと RADIUS 鍵を設定します。

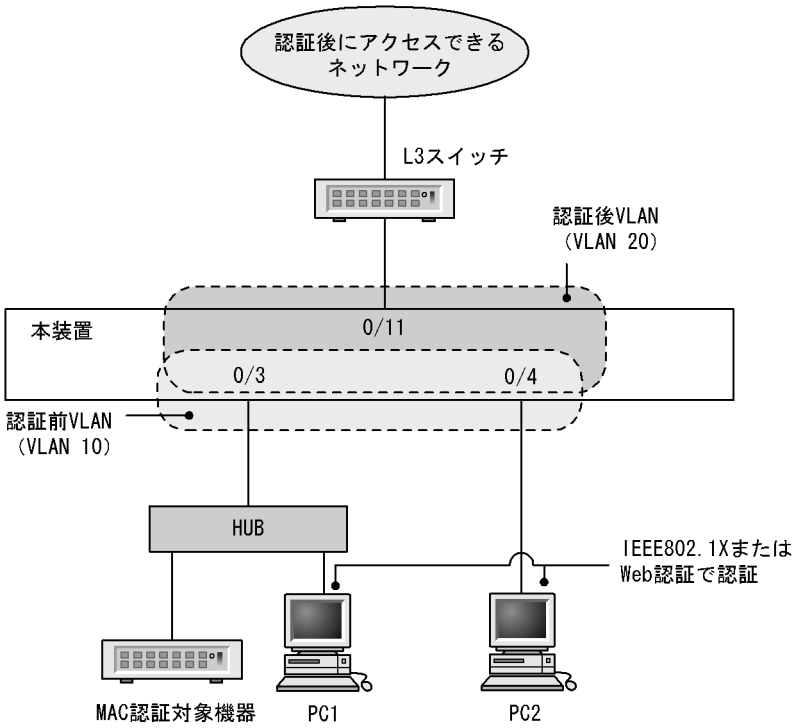
2. **(config)# mac-authentication system-auth-control**
   MAC 認証を起動します。

11.1.3 ダイナミック VLAN モードのコンフィグレーション

(1) ローカル認証方式の基本的な設定

ダイナミック VLAN モードで，認証方式を使用する上での基本的な設定を次の図に示します。

図 11-3 ダイナミック VLAN モードのローカル認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

MAC 認証で使用するポートを設定します。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 0/3-4**
   (config-if-range)# switchport mode mac-vlan
   (config-if-range)# switchport mac native vlan 10
   (config-if-range)# mac-authentication port
   (config-if-range)# exit
   認証を行う端末が接続されているポートに MAC 認証を設定します。

(b) MAC 認証の設定

[設定のポイント]

MAC 認証のコンフィグレーションコマンドを設定して MAC 認証を有効にします。

[コマンドによる設定]

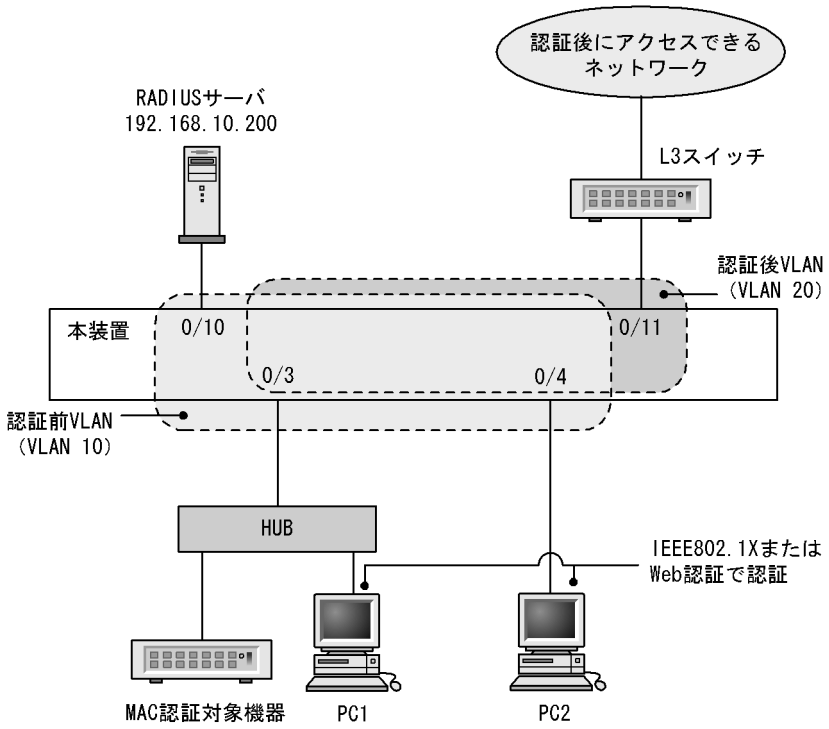
1. **(config)# mac-authentication system-auth-control**

MAC 認証を起動します。

(2) RADIUS 認証方式の基本的な設定

ダイナミック VLAN モードで，RADIUS 認証方式を使用する上での基本的な設定を次の図に示します。

図 11-4 ダイナミック VLAN モードの RADIUS 認証方式の基本構成



(a) 認証ポートの設定

[設定のポイント]

MAC 認証で使用するポートを設定します。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 0/3-4**
   (config-if-range)# switchport mode mac-vlan
   (config-if-range)# switchport mac native vlan 10
   (config-if-range)# mac-authentication port
   (config-if-range)# exit
   認証を行う端末が接続されているポートに MAC 認証を設定します。

(b) MAC 認証の設定

[設定のポイント]

MAC 認証のコンフィグレーションコマンドを設定して MAC 認証を有効にします。

[コマンドによる設定]

1. **(config)# aaa authentication mac-authentication default group radius**

```
(config)# mac-authentication radius-server host 192.168.10.200 key "macauth"
```
認証を RADIUS サーバでするために，IP アドレスと RADIUS 鍵を設定します。

2. **(config)# mac-authentication system-auth-control**
MAC 認証を起動します。

11.1.4 MAC 認証のパラメータ設定

MAC 認証で設定できるパラメータの設定方法を説明します。

(1) 認証最大時間の設定

[設定のポイント]

認証済みの端末を強制的に認証解除する時間を設定します。

[コマンドによる設定]

1. **(config)# mac-authentication max-timer 60**
強制的に認証解除する時間を 60 分に設定します。

(2) 固定 VLAN モードの認証数の設定

[設定のポイント]

固定 VLAN モードで認証できる MAC アドレス数を設定します。

[コマンドによる設定]

1. **(config)# mac-authentication static-vlan max-user 20**
MAC 認証の固定 VLAN モードで認証できる MAC アドレスの数を 20 個に設定します。

(3) RADIUS サーバの設定

[設定のポイント]

RADIUS 認証方式で使用する RADIUS サーバを設定します。

[コマンドによる設定]

1. **(config)# aaa authentication mac-authentication default group radius**
RADIUS サーバで認証するように設定します。

(4) アカウンティングの設定

[設定のポイント]

アカウンティング集計をするように設定します。

[コマンドによる設定]

1. **(config)# aaa accounting mac-authentication default start-stop group radius**
RADIUS サーバにアカウンティング集計をするように設定します。

(5) syslog サーバへの出力設定

[設定のポイント]

認証結果と動作ログを syslog サーバに出力する設定をします。

[コマンドによる設定]

1. **(config)# mac-authentication logging enable**
   (config)# logging event-kind aut
   MAC 認証の結果と動作ログを syslog サーバに出力する設定をします。

(6) 認証時に VLAN ID も照合する設定

[設定のポイント]

認証時に，MAC アドレスだけでなく VLAN ID も照合する場合に設定します。

[コマンドによる設定]

1. **(config)# mac-authentication vlan-check key "@@VLAN"**
   認証時に VLAN ID も照合します。
   また，RADIUS 認証方式で，MAC アドレスと VLAN ID とを “ @@VLAN ” の文字でつなげた文字列で RADIUS へ問い合わせます。

(7) RADIUS 問い合わせパスワードの設定

[設定のポイント]

RADIUS への照合の際に使用するパスワードを設定します。

[コマンドによる設定]

1. **(config)# mac-authentication password pakapaka**
   RADIUS への照合時のパスワードとして ” pakapaka ” を設定します。

(8) 認証失敗後の再認証時間間隔設定

[設定のポイント]

認証失敗後の次回認証までの再認証時間間隔を設定します。

[コマンドによる設定]

1. **(config)# mac-authentication auth-interval-timer 10**
   認証失敗後，10 分間経過後に再度認証を行うよう設定します。

(9) 認証専用 IPv4 アクセスリストの設定

[設定のポイント]

認証前状態の端末から特定のパケットを本装置外へ転送するよう設定します。

[コマンドによる設定]

1. **(config)# ip access-list extended 100**
   (config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 255.255.255.255 eq bootps

```
(config-ext-nacl)# permit udp 0.0.0.0 0.0.0.0 host 192.168.10.100 eq bootps
(config-ext-nacl)# exit
(config)# interface gigabitethernet 0/3
(config-if)# authentication ip access-group 100
(config-if)# exit
```

認証前の端末から DHCP パケットだけ 192.168.10.100 へのアクセスを許可する IPv4 アクセスリストを設定します。

(10) ダイナミック VLAN モードの認証数の設定

[設定のポイント]

ダイナミック VLAN モードで認証できる MAC アドレス数を設定します。

[コマンドによる設定]

1. `(config)# mac-authentication dynamic-vlan max-user 20`
   MAC 認証のダイナミック VLAN モードで認証できる MAC アドレスの数を 20 個に設定します。

(11) 端末からのアクセスがない状態を検出して認証解除する動作を無効に設定

[設定のポイント]

認証済み MAC アドレスを持つ端末からのアクセスがない状態が続いても認証を解除しないように設定します。

[コマンドによる設定]

1. `(config)# no mac-authentication auto-logout`
   認証済み MAC アドレスを持つ端末からのアクセスがない状態が続いても認証解除させない設定をします。

11.1.5 認証除外の設定方法

MAC 認証で認証対象外とするための設定を説明します。

(1) 固定 VLAN モードの認証除外ポートの設定

固定 VLAN モードで，認証しないで通信を許可するポートを次のように設定します。

[設定のポイント]

認証を除外するポートに対しては，認証ポートを設定しません。

[コマンドによる設定]

1.
```
(config)# vlan 10
(config-vlan)# state active
(config-vlan)# exit
(config)# interface gigabitethernet 0/4
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# mac-authentication port
```

```
(config-if)# exit
(config)# interface gigabitethernet 0/10
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# exit
```

固定 VLAN モードで扱う VLAN ID 10 を設定したポート 0/4 には認証ポートを設定します。また，ポート 0/10 には認証しないで通信を許可する設定をします。

(2) 固定 VLAN モードの認証除外端末の設定

固定 VLAN モードで，認証しないで通信を許可する端末の MAC アドレスを次のように設定します。

[設定のポイント]

認証を除外する端末の MAC アドレスを MAC アドレステーブルに登録します。

[コマンドによる設定]

1.
```
(config)# vlan 10
(config-vlan)# state active
(config-vlan)# exit
(config)# mac-address-table static 0012.e212.3456 vlan 10 interface
gigabitethernet 0/10
```

VLAN ID 10 のポート 0/10 に，認証しないで通信を許可する MAC アドレスを設定します。

(3) ダイナミック VLAN モードの認証除外ポートの設定

ダイナミック VLAN モードで，認証しないで通信を許可するポートを次のように設定します。

[設定のポイント]

認証を除外するポートに対しては，認証ポートを設定しません。

[コマンドによる設定]

1.
```
(config)# vlan 10
(config-vlan)# state active
(config-vlan)# exit
(config)# interface gigabitethernet 0/4
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 20
(config-if)# switchport mac native vlan 10
(config-if)# mac-authentication port
(config-if)# exit
(config)# interface gigabitethernet 0/10
(config-if)# switchport mode access
(config-if)# switchport access vlan 20
(config-if)# exit
```

ダイナミック VLAN モードで扱う MAC VLAN ID 20 を設定したポート 0/4 には認証ポートを設定します。また，ポート 0/10 には認証しないで通信を許可する設定をします。

(4) ダイナミック VLAN モードの認証除外端末の設定

ダイナミック VLAN モードで，認証しないで通信を許可する端末の MAC アドレスを次のように設定します。

[設定のポイント]

認証を除外する端末の MAC アドレスを，MAC VLAN と MAC アドレステーブルに登録します。

[コマンドによる設定]

1.
```
(config)# vlan 20 mac-based
(config-vlan)# mac-address 0012.e212.3456
(config-vlan)# exit
(config)# mac-address-table static 0012.e212.3456 vlan 20 interface
gigabitethernet 0/10
```
MAC VLAN ID 20 のポート 0/10 に，認証しないで通信を許可する端末の MAC アドレスを設定します。

(5) dot1q 設定 MAC ポートの認証除外設定

[設定のポイント]

dot1q 設定がされた MAC ポートの Tagged フレームを認証除外に設定します。

[コマンドによる設定]

1.
```
(config)# interface gigabitethernet 0/20
(config-if)# switchport mode mac-vlan
(config-if)# switchport mac vlan 20
(config-if)# switchport mac native vlan 10
(config-if)# switchport mac dot1q vlan 100
(config-if)# mac-authentication port
(config-if)# mac-authentication dot1q-vlan force-authorized
(config-if)# exit
```
MAC 認証の認証対象ポート 0/20 に受信した，VLAN ID 100 を持つ Tagged フレームを認証除外にする設定をします。

11.2 オペレーション

11.2.1 運用コマンド一覧

MAC 認証の運用コマンド一覧を次の表に示します。

表 11-2 運用コマンド一覧

コマンド名	説明
show mac-authentication login	MAC 認証で認証済みの MAC アドレスを表示します。
show mac-authentication logging	MAC 認証の動作ログ情報を表示します。
show mac-authentication	MAC 認証のコンフィグレーションを表示します。
show mac-authentication statistics	統計情報を表示します。
clear mac-authentication auth-state mac-address	認証済み端末を強制的に認証解除します。
clear mac-authentication logging	動作ログ情報をクリアします。
clear mac-authentication statistics	統計情報をクリアします。
set mac-authentication mac-address	内蔵 MAC 認証 DB へ MAC アドレスを登録します。
remove mac-authentication	内蔵 MAC 認証 DB から MAC アドレスを削除します。
commit mac-authentication	内蔵 MAC 認証 DB をフラッシュメモリに保存します。
show mac-authentication mac-address	内蔵 MAC 認証 DB に登録された情報を表示します。
store mac-authentication	内蔵 MAC 認証 DB をバックアップします。
load mac-authentication	バックアップファイルから内蔵 MAC 認証 DB を復元します。
clear mac-authentication dead-interval-timer	dead interval 機能による 2 台目以降の RADIUS サーバへのアクセスから，1 台目の RADIUS サーバへのアクセスに戻します。
restart mac-authentication	MAC 認証プログラムを再起動します。
dump protocols mac-authentication	MAC 認証のダンプ情報を収集します。

11.2.2 MAC 認証の設定情報表示

show mac-authentication コマンドで MAC 認証の設定情報が表示されます。

図 11-5 MAC 認証の設定情報表示

```
# show mac-authentication
Date 2008/10/17 10:52:49 UTC
mac-authentication Information:
   Authentic-method : RADIUS        Accounting-state    : disable
   Dead-interval    : 10
   Syslog-send      : enable
   Force-Authorized : enable
   Auth-max-user    : 1024

   Authentic-mode   : Static-VLAN
         Max-timer  : 60                  Max-terminal : 1024
         Port Count : 2                    Auto-logout : enable
   VLAN-check       : enable
         Vid-key    : %VLAN

   Authentic-mode   : Dynamic-VLAN
         Max-timer  : 60                  Max-terminal : 256
         Port Count : 2                    Auto-logout : enable

Port Information:
       Port               :    0/1
         Static-VLAN      :
            VLAN ID       :    5,10,15
            Auth type     :    force-authorized
         Dynamic-VLAN     :
            VLAN ID       :    1200,1500
            Native VLAN   :    10
            Forceauth VLAN:    1500
         Access-list-No   :    100
         Max-user         :    64

       Port               :    0/2
         Dynamic-VLAN     :
            VLAN ID       :    1300-1310
            Native VLAN   :    20
            Forceauth VLAN:    1300
         Access-list-No   :    100
         Max-user         :    64

       Port               :    0/10
         Static-VLAN      :
            VLAN ID       :    300,305
         Access-list-No   :    100
         Max-user         :    64
```

11.2.3 MAC 認証の統計情報表示

show mac-authentication statistics コマンドで MAC 認証の状態および RADIUS との通信状況が表示されます。

図 11-6 MAC 認証の表示

```
# show mac-authentication statistics
Date 2008/10/17 11:10:49 UTC
mac-authentication Information:
  Authentication Request Total :         100
  Authentication Current Count :          10
  Authentication Error Total   :          30
  Force Authorized Count       :          10
Unauthorized Information:
  Unauthorized Client Count    :           5
RADIUS mac-authentication Information:
[RADIUS frames]
           TxTotal   :       130  TxAccReq  :       130  TxError   :         0
           RxTotal   :       130  RxAccAccpt:       100  RxAccRejct:        30
                                  RxAccChllg:         0  RxInvalid :         0
Account mac-authentication Information:
[Account frames]
           TxTotal   :       100  TxAccReq  :       100  TxError   :         0
           RxTotal   :       100  RxAccResp :       100  RxInvalid :         0
Port Information:
  Port     User-count
   0/10      10/ 256
   0/12      10/1024
```

11.2.4 MAC 認証の認証状態表示

show mac-authentication login コマンドで MAC 認証の認証状態が表示されます。

図 11-7 MAC 認証の認証状態表示

```
# show mac-authentication login
Date 2008/10/17 10:52:49 UTC
Total client counts:2
F MAC address      Port   VLAN    Login time               Limit time  Mode
* 0012.e200.0001   0/1    3       2008/10/15 09:58:04 UTC  00:10:20    Static
* 0012.e200.0002   0/10   4094    2008/10/15 10:10:23 UTC  00:20:35    Dynamic
```

11.2.5 内蔵 MAC 認証 DB の作成

MAC 認証システムの環境設定およびコンフィグレーションの設定が完了したあとに，内蔵 MAC 認証 DB を作成します。また，すでに内蔵 MAC 認証 DB に登録されている内容を修正します。

(1) MAC アドレスの登録

set mac-authentication mac-address コマンドで，認証対象の MAC アドレスごとに MAC アドレス，VLAN ID を登録します。MAC アドレスを五つ登録する例を次に示します。

[コマンド入力]

```
# set mac-authentication mac-address 0012.e200.1234 100
# set mac-authentication mac-address 0012.e200.5678 100
# set mac-authentication mac-address 0012.e200.9abc 100
# set mac-authentication mac-address 0012.e200.def0 100
# set mac-authentication mac-address 0012.e200.0001 100
```

(2) MAC アドレス情報削除

登録済み MAC アドレスを削除します。

[コマンド入力]

```
# remove mac-authentication mac-address 0012.e200.1234
```

MAC アドレス (0012.e200.1234) を削除します。

(3) 内蔵 MAC 認証 DB への反映

commit mac-authentication コマンドで，set mac-authentication mac-address コマンドおよび remove mac-authentication mac-address コマンドで登録・削除した情報を，内蔵 MAC 認証 DB に反映します。

[コマンド入力]

```
# commit mac-authentication
```

11.2.6 内蔵 MAC 認証 DB のバックアップ

内蔵 MAC 認証 DB のバックアップ方法，およびバックアップファイルからの復元方法を次に示します。

(1) 内蔵 MAC 認証 DB のバックアップ

内蔵 MAC 認証 DB から store mac-authentication コマンドでバックアップファイル（次の例では backupfile）を作成します。

[コマンド入力]

```
# store mac-authentication backupfile
Backup mac-authentication MAC address data.  Are you sure? (y/n): y
#
```

(2) 内蔵 MAC 認証 DB の復元

バックアップファイル（次の例では backupfile）から load mac-authentication コマンドで内蔵 MAC 認証 DB を作成します。

[コマンド入力]

```
# load mac-authentication backupfile
Restore mac-authentication MAC address data.  Are you sure? (y/n): y
#
```

11.2.7 dead interval 機能による RADIUS サーバアクセスを 1 台目の RADIUS サーバに戻す

1 台目の RADIUS サーバが無応答になり，dead interval 機能によって，2 台目以降の RADIUS サーバへのアクセスに切り替わった場合，コンフィグレーションコマンド authentication radius-server dead-interval で設定された時間を待たないで最初の RADIUS サーバへのアクセスに戻すには，clear mac-authentication dead-interval-timer コマンドを実行します。

図 11-8 1 台目の RADIUS サーバへの切り替え

```
# clear mac-authentication dead-interval-timer
#
```

12 認証 VLAN【OP-VAA】

認証 VLAN は，専用の認証サーバと連携してユーザ単位に VLAN へのアクセス制御を行う VLANaccessAgent と呼ばれる機能です。
この章では，認証 VLAN の解説と操作方法について説明します。

12.1 解説

認証 VLAN は，専用の認証サーバと連携してユーザ単位に VLAN へのアクセス制御を行う VLANaccessAgent と呼ばれる機能です。本装置配下に接続された端末から認証サーバに対してログインを行い，ユーザ認証が行われた結果，認証情報が本装置に通知されます。本装置は，送られてきた情報中の MAC アドレスを用いて，所定の VLAN に組み込むことによって，所属する VLAN の収容切り替えを行います。

また，本装置での認証有無にかかわらず，認証サーバから通知された認証情報をすべて登録する「通常モード」と，本装置で認証された MAC アドレスだけを登録する「スイッチ間非同期モード」があります。

認証 VLAN は，NEC 統合システム運用管理製品（WebSAM）の VLANaccess と呼ばれる認証 VLAN 専用ソフトウェアをインストールした 1 台以上の認証サーバと本装置とで構成されます。

また，認証を行う端末には，認証 VLAN ログオンと Windows ドメインログオンを SingleSignOn することができる VLANaccessClient と呼ばれる PC 上の専用クライアントソフトウェアを使用します。なお，専用クライアントソフトウェアを使用しないで，Web ブラウザで認証を行うこともできます。ただし，スイッチ間非同期モードを使用する場合は Web ブラウザとして Internet Explorer 6.0 を使用してください。

認証サーバにインストールされているソフトウェアを次の表に示します。

表 12-1 認証サーバにインストールされているソフトウェア

ソフトウェア名称		概説	接続可能な装置の動作モード	
			通常モード	スイッチ間非同期モード
VLANaccess2.0	NEC VitalQIP	統合的な IP アドレス管理を行います（運用管理機能，DNS サーバ，DHCP サーバを含みます）。	○	×
	NEC VitalQIP Registration Manager	DHCP 環境での Web によるユーザアクセス認証を行います。		
	VLANaccessController	VLANaccessAgent との通信および認証 Web アドオン機能で構成されています。		
VLANaccessController Ver.3.0 以降		Windows 2000 Server SP4 または，Windows 2003 Server の Active Directory と連携して，VLANaccessAgent との通信を行います。	○	○

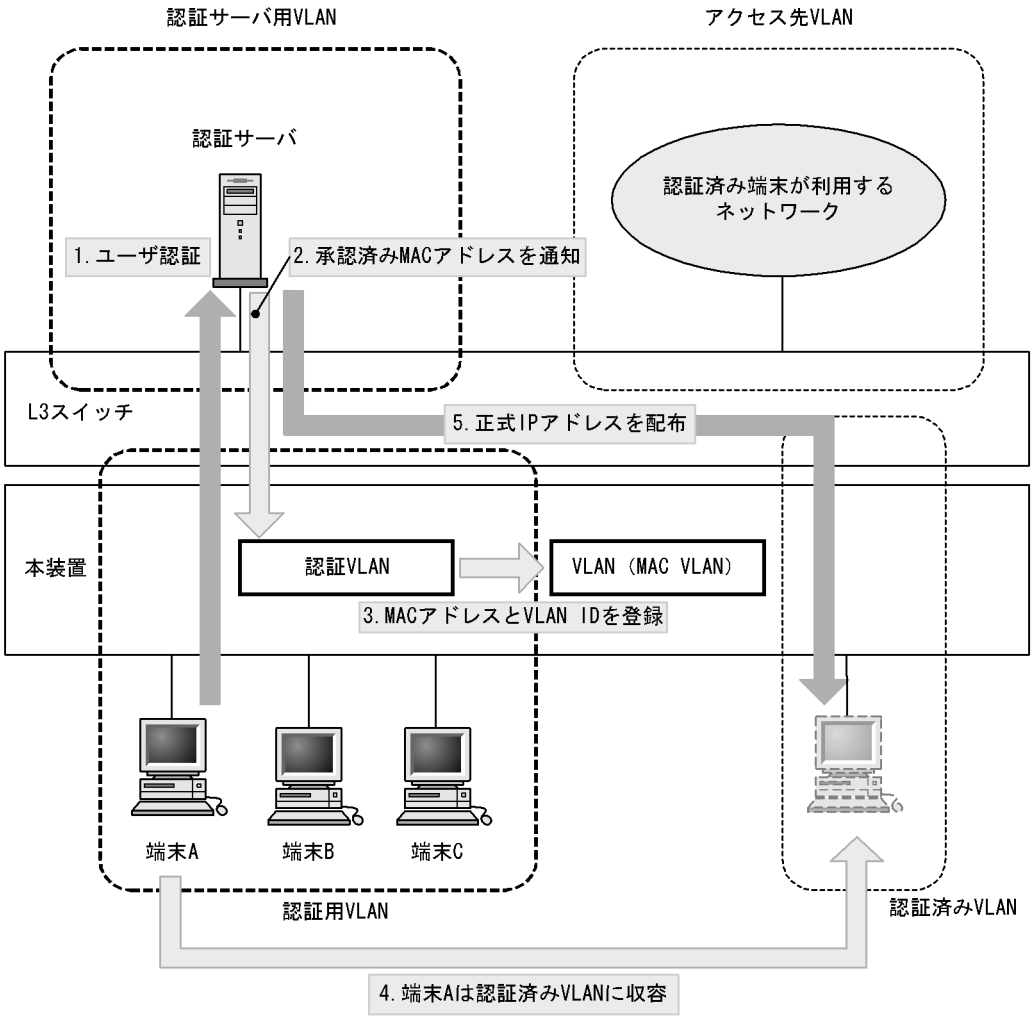
（凡例）○：接続可能　　×：接続不可

認証 VLAN は，本装置の配下に一般の L2 スイッチが使用でき，システム構築に自由度があります。

12.1.1 機能概要

本装置を使った認証 VLAN の基本構成を次の図に示します。

図 12-1　認証 VLAN 基本構成



（凡例）
認証用VLAN　　：未承認のユーザ端末に割り当てるVLAN
認証済みVLAN　：ユーザ認証が完了したあとに端末に割り当てるVLAN
認証サーバ用VLAN：認証サーバを接続するVLAN
アクセス先VLAN　：認証後に端末が実際にアクセスするVLAN

12.1.2　認証手順

認証は，「図 12-1　認証 VLAN 基本構成」に示した手順で行われます。

1. **ユーザ認証**
   認証を受ける端末は事前に DHCP クライアントの設定を行います。認証サーバ内の DHCP サーバ機能から認証サーバとの接続に使用する IP アドレスが端末に配布され，認証サーバで認証を受けることができます。
2. **認証済み** MAC **アドレス通知**
   認証完了後，認証サーバから MAC アドレスと VLAN 情報が本装置に通知されます。
3. MAC **アドレスと** VLAN ID **を登録**
   認証サーバから通知された端末の MAC アドレスを，指定された VLAN に登録します。

4. **認証済み VLAN に収容**
   該当する MAC アドレスを持つ端末を認証済み VLAN に収容します。

5. **端末に正式 IP アドレス配布**
   認証サーバ内の DHCP サーバ機能から正式な IP アドレスが端末に配布されます。

また，ユーザがログアウトを行うと認証サーバのログアウト処理で MAC アドレスが本装置に通知され，認証用 VLAN に収容を戻します。

12.1.3 認証 VLAN で使用する VLAN

認証 VLAN を使用するために必要な設定を「表 12-2　認証 VLAN に必要な VLAN 設定」に示します。

なお，認証を行う端末が接続されているポートには，ポート VLAN のコンフィグレーションと MAC VLAN のコンフィグレーションの両方が必要です。

表 12-2　認証 VLAN に必要な VLAN 設定

種別	VLAN 設定	用途
認証用 VLAN	ポート VLAN	認証対象で認証を受ける端末を収容する VLAN
認証済み VLAN	MAC VLAN	認証後に収容する VLAN
認証サーバ用 VLAN	ポート VLAN	認証サーバを収容する VLAN
アクセス先 VLAN	ポート VLAN	端末が実際にアクセスするネットワークの VLAN

また，認証 VLAN を使用するにあたっては，VLAN 間で次のフィルタ設定が必要となります。

認証用 VLAN と認証済み VLAN 間：
　全 IP 通信ができないようにフィルタを設定します。

認証用 VLAN と認証サーバ用 VLAN 間：
　HTTP，DHCP，ICMP の通信だけ中継するようにフィルタを設定します。

認証用 VLAN とアクセス先 VLAN 間：
　全 IP 通信ができないようにフィルタを設定します。

認証済み VLAN と認証サーバ用 VLAN 間：
　HTTP，DHCP，ICMP の通信だけ中継するようにフィルタを設定します。

認証済み VLAN とアクセス先 VLAN 間：
　フィルタ設定を行いません（すべての IP 通信を許可します）。

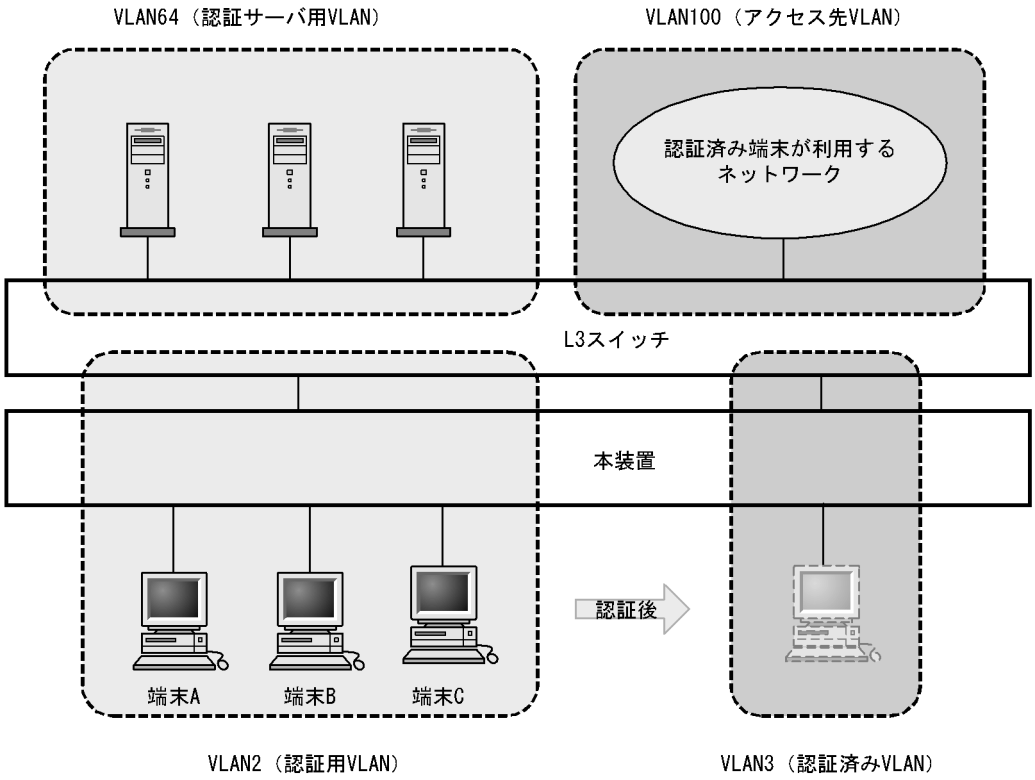
認証サーバ用 VLAN とアクセス先 VLAN 間：
　全 IP 通信ができないようにフィルタを設定します。

12.1.4 認証 VLAN の応用構成

(1) 認証サーバの複数台構成

認証サーバは 10 台まで設定できます。複数の認証サーバを設定することによって，認証時のサーバの負荷を分散できます。認証サーバを複数台使用した認証 VLAN の構成例を次の図に示します。

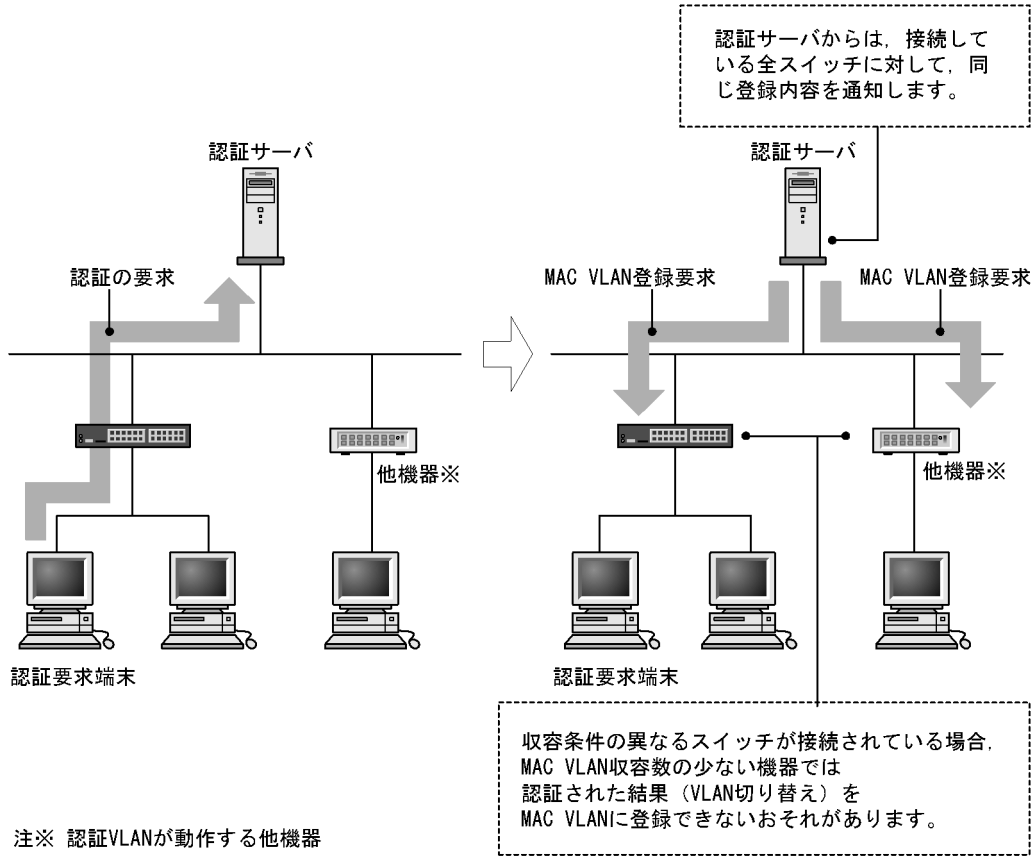
図 12-2 認証サーバ複数台構成



12.1.5 スイッチ間非同期モード

認証サーバで認証されたあと，認証サーバ配下の全認証スイッチに対して認証済み MAC アドレスの登録要求が出されますが，認証サーバ上の認証データがスイッチの収容条件を超えている場合，通常モードでは，認証された MAC アドレスが MAC VLAN に登録できない状態が発生することがあります。通常モードでの動作を次の図に示します。

図 12-3 通常モードでの動作

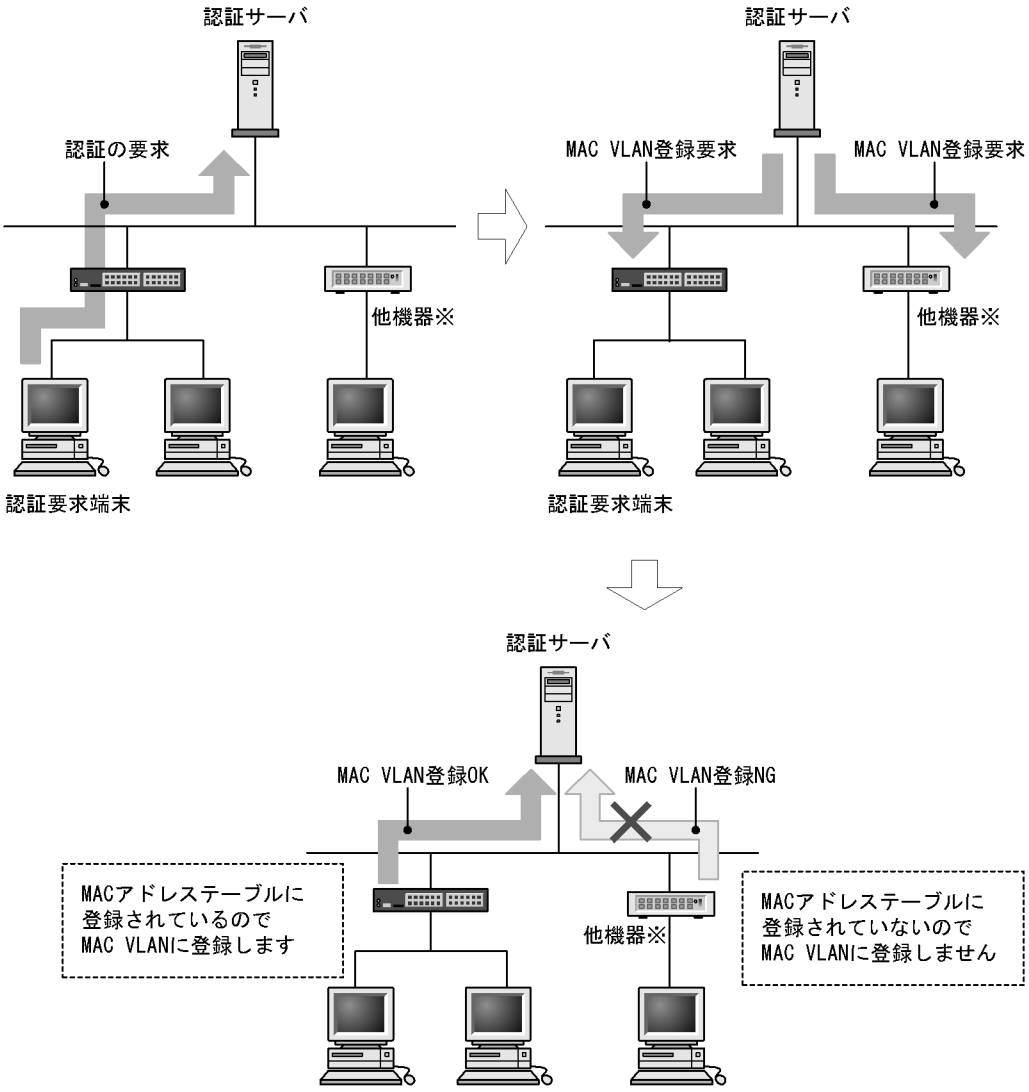


この問題を解決するためには，コンフィグレーションコマンド no fense vaa-sync を設定して，スイッチ間非同期モードを有効にします。スイッチ間非同期モードでは，「図 12-4 認証対象端末だけの登録」に示すように，認証要求を行う端末を収容しているスイッチの MAC アドレステーブルに対象の MAC アドレスが登録されている場合だけ，MAC VLAN の MAC アドレスを登録します。認証要求端末を収容していないスイッチには MAC アドレスを登録しません。（認証サーバでは，MAC VLAN 登録完了通知が一つ受信できれば，その端末は認証したものとみなされます。）

スイッチ間非同期モードを有効とした場合，ほかのスイッチの MAC VLAN の収容条件によらずに，スイッチの収容能力まで認証できますが，「12.1.6 認証 VLAN 使用上の注意 （11）スイッチ間非同期モード有効時の注意」に示す制限があります。

なお，コンフィグレーションコマンド fense vaa-sync が設定（デフォルト設定）されている場合は，通常モードの動作を行います。

図 12-4 認証対象端末だけの登録



注※ 認証VLANのスイッチ間非同期モードが動作する他機器

12.1.6 認証 VLAN 使用上の注意

(1) IEEE802.1X 認証との共存について

IEEE802.1X 認証が動作している場合（コンフィグレーションコマンド dot1x system-auth-control を実行している場合），認証 VLAN を同時に使用することはできません。

(2) 無線 LAN 使用について

本装置の配下に無線 LAN を使用する際は，アクセスポイントのルータの設定および DHCP サーバの設定を必ず OFF にしてください。

(3) 認証サーバで VLANaccess2.0 を使用する場合の注意

認証サーバで VLANaccess2.0 を使用する場合，Microsoft Windows 2000 Server に実装されている次のサービスを必ず停止してください。

- DHCP サーバ
- DHCP クライアント
- DNS サーバ

(4) エージングタイムの設定について

認証 VLAN を使用する場合，MAC アドレステーブルエントリのエージングタイムに 0（無限）を設定しないでください。0 を設定すると，認証後に VLAN が切り替わったとき，切り替わる前の VLAN の MAC アドレステーブルエントリがエージングされずに残ってしまうため，不要な MAC アドレステーブルエントリが蓄積することになります。

なお，切り替える前の VLAN に不要な MAC アドレステーブルエントリが蓄積した場合は，運用コマンド clear mac-address-table で消去してください。

(5) mac-address コマンドで静的 MAC アドレスを登録する場合の注意

（config-vlan）モード時にコンフィグレーションコマンド mac-address で静的 MAC アドレスを登録する場合，認証対象となる端末の MAC アドレスが指定されると認証済み VLAN に移動できなくなりますので，指定しないでください。

(6) no fense server コマンド実行時の動作について

コンフィグレーションコマンド no fense server を実行すると，対応する認証サーバとの接続を切断しますが，すでに認証された MAC アドレスはそのままの状態ですので，認証済み端末からの通信を続けられます。さらに，コンフィグレーションコマンド fense server の実行によって認証サーバとの接続を再開しても，認証済み端末は再認証を行わずに通信を続けられます。認証サーバとの接続が切断された状態のまま放置してしまうと認証済み端末が不用意に使用されるおそれがありますので，このような場合は，本装置の認証 VLAN を運用コマンド restart vaa で再起動して，認証済み端末の MAC アドレスを削除してください。

(7) 認証サーバ設定時および認証 VLAN コンフィグレーション変更時の注意

認証サーバのネットワーク設定の変更，認証 VLAN のコンフィグレーションコマンド fense vaa-name，fense server および fense vlan で認証 VLAN システムのネットワーク構成を変更した場合，またはコンフィグレーションコマンド no fense server で認証 VLAN をいったん停止して，再度コンフィグレーションコマンド fense server で起動した場合は，必ず認証サーバの VLANaccessController を含む認証 VLAN 関連の各機能を再起動して，さらに，本装置の認証 VLAN を再起動してください。

なお，認証サーバの各機能の再起動については，認証サーバソフトに添付される説明書を参照してください。

(8) 認証サーバの HCInterval と fense alive-timer の推奨する設定値

認証 VLAN の安定動作のため，認証端末数に従って，コンフィグレーションおよび認証サーバの設定パラメータの値（fense.conf）を設定してください。推奨する値を次の表に示します。

表 12-3 コンフィグレーション，認証サーバの設定パラメータの値

認証端末数	コンフィグレーション	認証サーバの設定パラメータ	
	fense alive-timer	HCInterval	RecvMsgTimeout
1 ～ 256	20 秒（デフォルト）	15 秒（デフォルト）	20 秒（デフォルト）

（9） 認証サーバとの接続 / 切断が頻繁に発生する場合

認証 VLAN のコンフィグレーションコマンド設定変更によって認証サーバとの接続／切断を繰り返す場合があります。このような場合は，認証サーバ側の VLANaccessController を含む認証 VLAN の各機能を再起動してください。

（10） 動的 MAC アドレスの解放契機について

次の動作を行った場合，認証 VLAN が MAC VLAN に登録した動的 MAC アドレスを解放するため，端末から認証済み VLAN への通信ができなくなります。

- VLANaccessAgent を停止する。
- 認証 VLAN をログアウトする。

また，次の動作を行った場合，動的 MAC アドレスを一時的に解放しますが，認証サーバとのセッションが再接続されたあとに動的 MAC アドレスを再登録するので，端末から認証済み VLAN への通信を継続できます。

- 運用コマンド restart vaa で VLANaccessAgent を再起動する。
- 運用コマンド restart vlan mac-manager で L2MAC 管理機能を再起動する。

（11） スイッチ間非同期モード有効時の注意

スイッチ間非同期モードを有効とした場合，次に示す制限事項があります。

- 一度認証した端末がほかのスイッチに移動した場合は，再度認証操作が必要となります。
- GSRP で装置冗長構成を組んだ場合に装置切り替えが発生すると，再度認証操作が必要となります。
- 認証端末が収容されているかの判断に MAC アドレステーブルを利用しているので，認証前 VLAN の MAC アドレステーブルがクリアされると，認証が失敗してしまいます。
- 本機能を実行しているスイッチと同一のサブネットに，通常モードの認証 VLAN が動作しているスイッチを混在させないでください。認証対象端末が接続されていなくても，通常モードの認証 VLAN が動作しているスイッチから認証サーバに登録完了の通知が届いてしまい，認証サーバ上の認証情報に不一致が発生する場合があります。
- 認証サーバに認証済みの MAC アドレスが保持されていても，スイッチが再起動すると MAC アドレステーブルをクリアしますので，スイッチ再起動後に認証が解除される場合があります。

（12） MAC VLAN コンフィグレーションコマンド mac-based-vlan static-only コマンド設定時の注意

MAC VLAN のコンフィグレーションコマンド mac-based-vlan static-only が設定された場合，認証 VLAN は設定できません。

12.2 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

認証 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 12-4 コンフィグレーションコマンド一覧

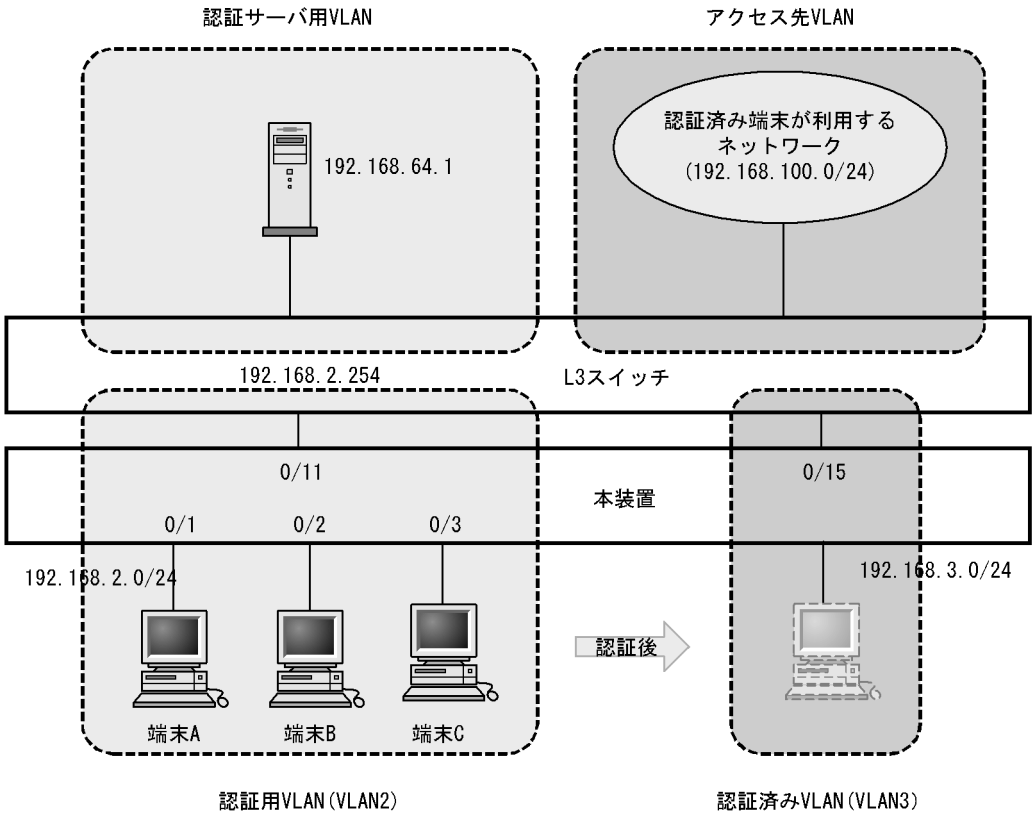
コマンド名	説明
fense alive-timer	VLANaccessController からの KeepAlive パケットの監視時間を設定します。
fense retry-count	登録済み動的 MAC アドレスを削除するまでの VLANaccessController との接続リトライ回数を設定します。
fense retry-timer	VLANaccessController との接続リトライ間隔を設定します。
fense server	VLANaccessController の IP アドレス，TCP ポート番号を指定します。
fense vaa-name	VLANaccessAgent の名称を設定します。
fense vaa-sync	通常モード／スイッチ間非同期モードを設定します。
fense vlan	認証済み VLAN の VLAN ID およびサブネットを指定します。

12.2.2 認証 VLAN の基本的な設定

認証 VLAN を使用する上での基本的な設定を説明します。

本装置と認証サーバ 1 台でシステムを構成した場合の構成図を次の図に示します。

図 12-5 認証 VLAN 基本構成



認証用 VLAN と認証済み VLAN を設定したあと，VLANaccessAgent の名称を設定し，VLANaccessController の IP アドレス，認証済み VLAN の VLAN ID，サブネットを設定します。

さらに，L3 スイッチ側に各 VLAN 間のフィルタ設定と，認証用 VLAN および認証済み VLAN からサーバ用 VLAN への DHCP リレーを設定します。

(1) デフォルト経路の設定

[設定のポイント]

本装置のデフォルト経路に，L3 スイッチのインタフェースアドレスを設定します。

[コマンドによる設定]

1. **(config)# ip default-gateway 192.168.2.254**

   上位 L3 スイッチの認証用 VLAN の IP アドレスを，本装置のデフォルト経路に設定します。

(2) 認証ポートの設定

[設定のポイント]

認証を行う端末が接続されているポート 0/1-3 に，認証用 VLAN と認証済み VLAN を指定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1-3**
   (config-if)# switchport mode mac-vlan

```
(config-if)# switchport mac vlan 3
(config-if)# switchport mac native vlan 2
```

ポート 0/1-3 に MAC VLAN（VLAN3）と native vlan（VLAN2）を設定します。

(3) 認証 VLAN の設定

[設定のポイント]

認証 VLAN のコンフィグレーションコマンドを設定して認証 VLAN を有効にします。

[コマンドによる設定]

1. `(config)# fense vaa-name switch01`
   本装置の VLANaccessAgent の名称を設定します。

2. `(config)# fense 1 vlan 10 192.168.3.0 255.255.255.0`
   認証済み VLAN のサブネットを設定します。

3. `(config)# fense 1 server 192.168.64.1`
   VLANaccessController の IP アドレスを設定します。

12.2.3 認証 VLAN のパラメータ設定

認証 VLAN で可能なパラメータ設定を説明します。

(1) 認証サーバ接続リトライ間隔の設定

[設定のポイント]

認証サーバとの接続リトライ間隔を設定します。

[コマンドによる設定]

1. `(config)# fense 1 retry-timer 30`
   VAA ID 1 の VLANaccessAgent に接続リトライ間隔を 30 秒に設定します。

(2) MAC アドレス削除接続リトライ回数の設定

[設定のポイント]

本装置に登録済みの MAC アドレスを削除するまでの認証サーバとの接続リトライ回数を設定します。

[コマンドによる設定]

1. `(config)# fense 1 retry-count 10`
   VAA ID 1 の VLANaccessAgent に MAC アドレスを削除するまでの接続リトライ回数を 10 回に設定します。

(3) KeepAlive パケット監視時間間隔の設定

[設定のポイント]

VLANaccessController からの KeepAlive パケットがこのコマンドで設定した時間以内に到着しない

場合，認証サーバへの再接続処理を実行します。

［コマンドによる設定］

1. **(config)# fense 1 alive-timer 40**
   VAA ID 1 の VLANaccessAgent に認証サーバからの KeepAlive パケット受信を待つ時間を 40 秒に設定します。

（4） スイッチ間非同期モードの設定

［設定のポイント］

装置のスイッチ間非同期モードを有効にします。

［コマンドによる設定］

1. **(config)# no fense vaa-sync**
   スイッチ間非同期モードを有効にします。

12.3 オペレーション

12.3.1 運用コマンド一覧

認証 VLAN の運用コマンド一覧を次の表に示します。

表 12-5 運用コマンド一覧

コマンド名	説明
show fense server	VLANaccessAgent の情報を表示します。
show fense statistics	VLANaccessAgent の統計情報を表示します。
show fense logging	VLANaccessAgent のログ情報を収集し表示します。
clear fense statistics	VLANaccessAgent の統計情報をクリアします。
clear fense logging	VLANaccessAgent のログ情報をクリアします。
restart vaa	VLANaccessAgent プログラムを再起動します。
dump protocols vaa	VLANaccessAgent のダンプ情報を収集します。

12.3.2 認証 VLAN 動作確認

認証 VLAN を使用した場合，show fense server detail コマンドを実行して動作の確認を行ってください。

図 12-6 認証 VLAN 詳細状態情報表示

```
> show fense server detail
Date 2006/05/01 10:50:49 UTC
VAA NAME: switch01
VAA Sync Mode: Sync
Current Registered MAC:  120                                          … 1
Server Information:
ID:1          Status: enable           Agent Status: CONNECTED        … 2,3
      Server Address: 192.168.2.100            Port: 52153
         Retry Timer:    10  Retry Count: 25920     Current Count:          0
         Alive Timer:    20
   Target-VLAN Count:     4
   Target-VLAN Information:
          VLAN ID:2    lP Subnet Address: 192.168.2.0     mask 255.255.255.0
          VLAN ID:3    lP Subnet Address: 192.168.3.0     mask 255.255.255.0
          VLAN ID:4    lP Subnet Address: 192.168.4.0     mask 255.255.255.0
          VLAN ID:10   lP Subnet Address: 192.168.10.0    mask 255.255.255.0
```

[確認ポイント]

1. Current Registered MAC
   MAC VLAN に登録済みの MAC アドレス数です。登録されている MAC アドレスの一覧を表示する場合は，show vlan mac-vlan <vlan id list> dynamic コマンドを使用してください。
2. Status
   <vaa_id> ごとの起動 / 停止状態を表します。enable であることを確認してください。
3. Agent Status
   認証サーバとの接続状態が CONNECTED であることを確認してください。

13 DHCP snooping

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，IPv4 ネットワークに適用します。
この章では，DHCP snooping の解説と操作方法について説明します。

13.1　解説

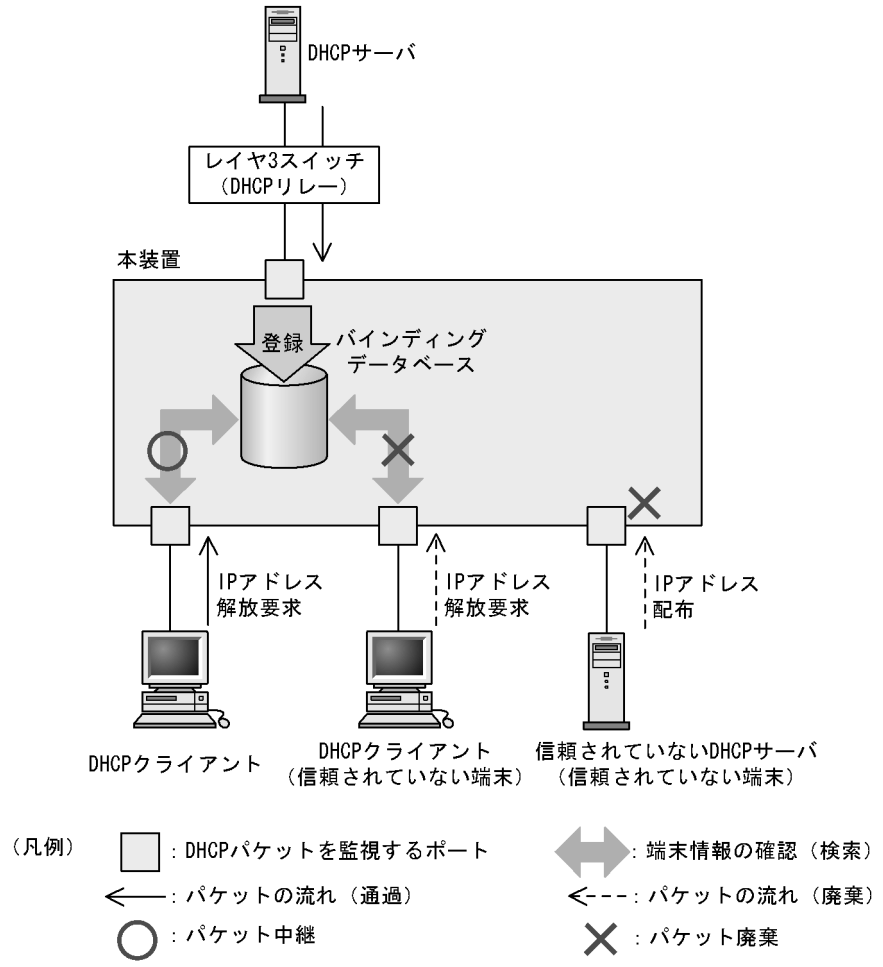
13.1.1　概要

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。

また，信頼されていない端末からの IPv4 パケットを制限する端末フィルタや，不正な ARP パケットを廃棄するダイナミック ARP 検査もサポートしています。

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 13-1　DHCP snooping 概要



端末情報の登録先をバインディングデータベースと呼びます。

DHCP snooping でサポートする機能を次の表に示します。

表 13-1 DHCP snooping でサポートする機能

項目	機能の概要
DHCP パケットの監視	• DHCP サーバから IP アドレスを配布された DHCP クライアントを監視し，端末情報をバインディングデータベースで管理
固定 IP アドレスを持つ端末の登録	• バインディングデータベースへ端末情報をスタティックに登録
バインディングデータベースの保存	• 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
DHCP パケットの検査	• 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 • 信頼されていない DHCP クライアントからの IP アドレス解放を抑止 • MAC アドレスの詐称を抑止 • Option82 の詐称を抑止
DHCP パケットの受信レート制限	• 設定した受信レートを超えた DHCP パケットを廃棄
端末フィルタ	• 信頼されていない端末からの IPv4 パケットの中継を抑止
ARP パケットの検査	• 信頼されていない端末からの ARP パケットの中継を抑止 • MAC アドレスおよび IP アドレスの詐称を抑止
ARP パケットの受信レート制限	• 設定した受信レートを超えた ARP パケットを廃棄

13.1.2 DHCP パケットの監視

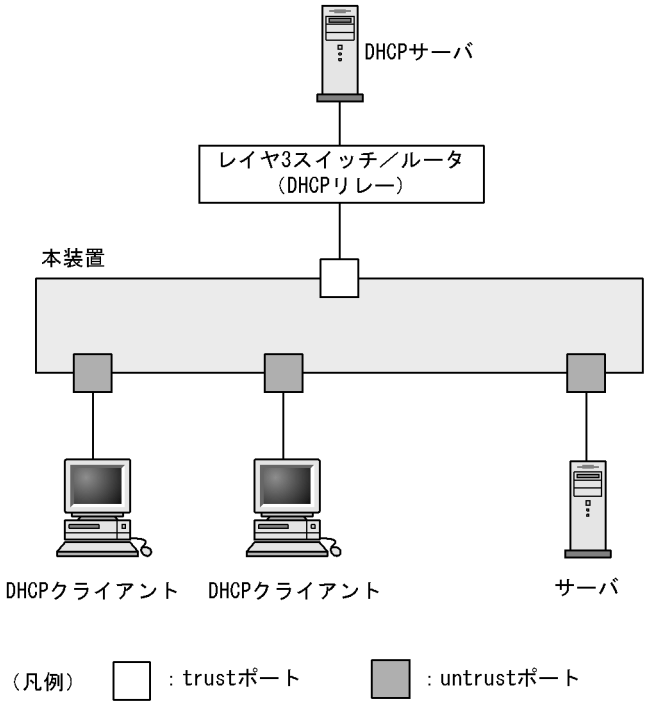
(1) ポートの種別

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

- trust ポート
  DHCP サーバや部門サーバなど，信頼済みの端末を接続するポートを trust ポートと呼びます。
- untrust ポート
  DHCP クライアントなど，信頼されていない端末を接続するポートを untrust ポートと呼びます。
  DHCP サーバは接続しません。

ポートの種別を次の図に示します。

図 13-2 ポートの種別



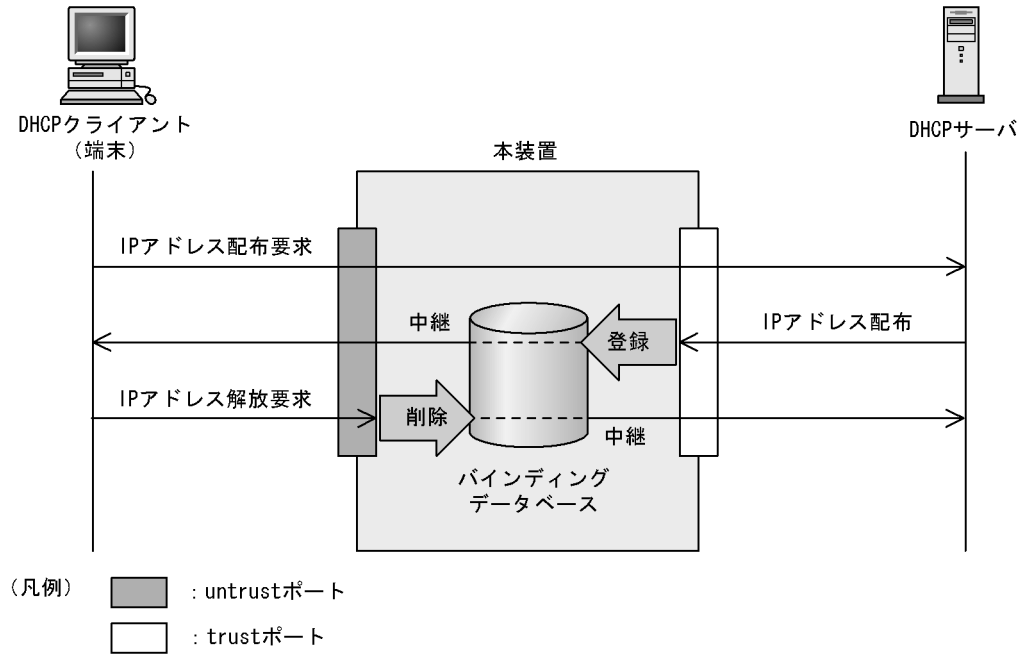
コンフィグレーションコマンド ip dhcp snooping で DHCP snooping を有効にすると，デフォルトですべてのポートが untrust ポートになります。DHCP サーバへ接続するポートを trust ポートとして設定してください。trust ポートはコンフィグレーションコマンド ip dhcp snooping trust で設定できます。

なお，DHCP snooping では，コンフィグレーションコマンド ip dhcp snooping vlan で指定した VLAN を監視対象にします。

(2) 端末情報の学習

端末情報の学習の動作概要を次の図に示します。

図 13-3 端末情報の学習の動作概要



trust ポートでは，受信した DHCP サーバからのパケットを監視し，IP アドレスが配布された場合にはバインディングデータベースに端末情報を登録します。

untrust ポートでは，受信した DHCP クライアントからのパケットを監視し，IP アドレスの解放要求の場合にはバインディングデータベースから端末情報を削除します。

バインディングデータベースの登録には，次の二つの種類があります。

- 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します。
  通常は，ダイナミック登録によって端末情報を登録します。
- 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 で登録します。
  スタティック登録は，untrust ポートに固定 IP アドレスを持つ部門サーバなどを接続するときに利用します。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。

バインディングデータベースに登録する端末情報を次の表に示します。

表 13-2 バインディングデータベースに登録する端末情報

項目	ダイナミック登録	スタティック登録
端末の MAC アドレス	DHCP クライアントの MAC アドレス	固定 IP アドレスを持つ端末の 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 アドレスを持つ端末の IP アドレス
	次に示す範囲が有効 • 1.0.0.0 ～ 126.255.255.255 • 128.0.0.0 ～ 223.255.255.255	
端末が所属する VLAN	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	
端末を接続するポート番号	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	

項目	ダイナミック登録	スタティック登録
エージング時間	エージングによってエントリを削除するまでの時間 なお，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

(3) 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の設定によって，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できます。

(a) 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を保存するには，コンフィグレーションコマンド ip dhcp snooping database url を設定します。

実際に保存が開始されるのは，コンフィグレーションで設定された書き込み待ち時間満了時です。

(b) 書き込み待ち時間満了時の保存

書き込み待ち時間とは，バインディングデータベース保存時の，保存契機から書き込むまでの待ち時間です。次のどれかを保存契機としてタイマを開始し，タイマが満了した時点で指定した保存先へ保存します。

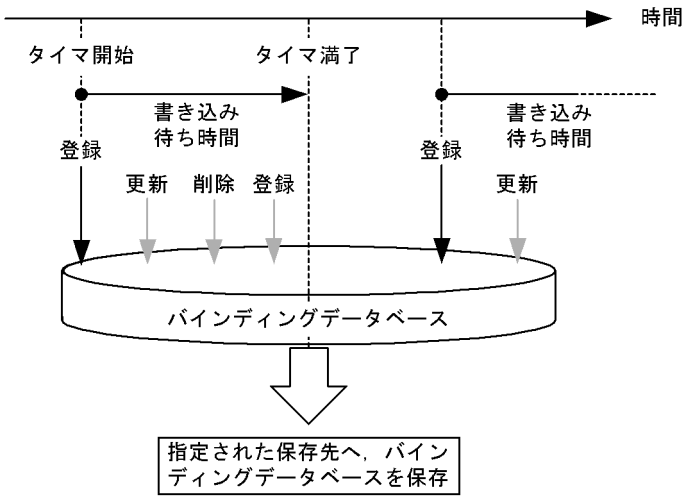
- ダイナミックのバインディングデータベースの登録，更新，または削除時
- コンフィグレーションコマンド ip dhcp snooping database url 設定時（保存先の変更を含む）
- 運用コマンド clear ip dhcp snooping binding 実行時

書き込み待ち時間は，コンフィグレーションコマンド ip dhcp snooping database write-delay で設定できます。

これらの保存契機で書き込み待ち時間のタイマを開始すると，タイマ満了までタイマは停止しません。この間にバインディングデータベースの登録，更新，または削除が発生してもタイマは再開始しません。

保存契機と書き込み待ち時間との関係を次の図に示します。なお，この図ではバインディングデータベースへの登録を保存契機としています。

図 13-4 保存契機と書き込み待ち時間との関係



(c) バインディングデータベースの保存先

保存先には，内蔵フラッシュメモリと MC のどちらかを選択できます。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。

保存対象は，書き込み時点の全エントリです。また，次の書き込み時には上書きされます。

(d) 保存したバインディングデータベースの復元

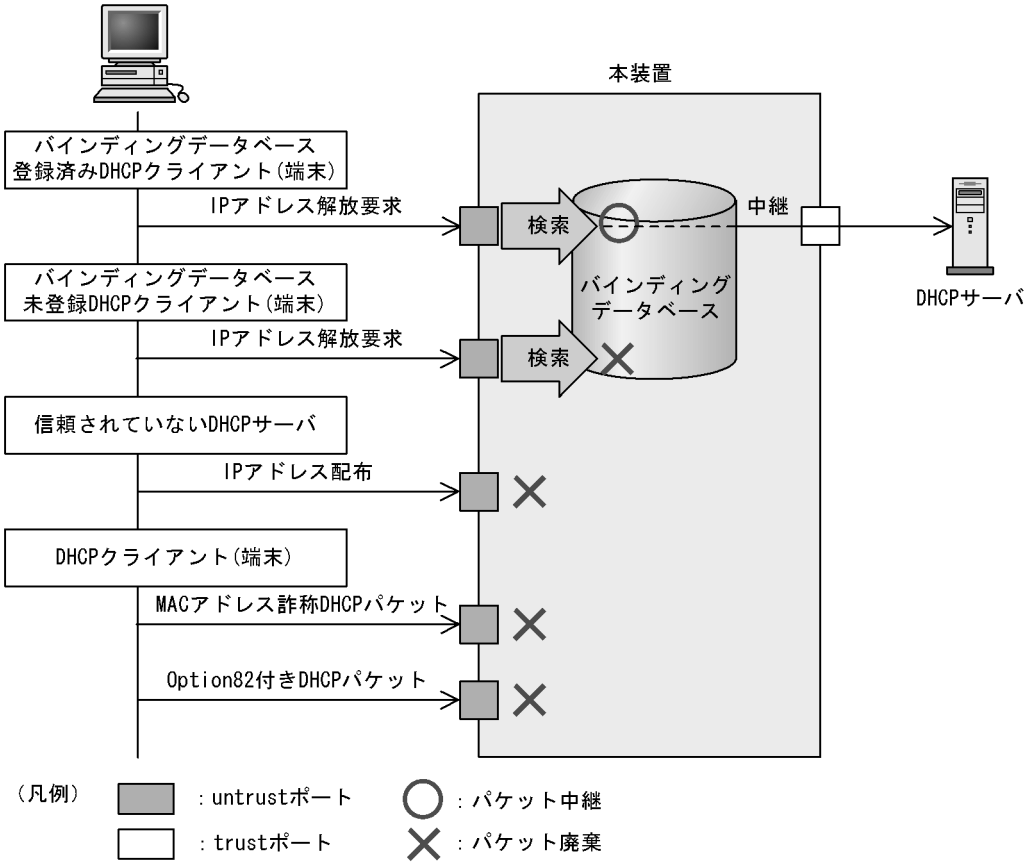
保存したバインディングデータベースは，装置起動時に復元します。復元には，装置起動時に次の条件をどちらも満たしている必要があります。

- 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

(4) DHCP パケットの検査

DHCP パケット検査の動作概要を次の図に示します。

図 13-5 DHCP パケット検査の動作概要



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，次に示すアクセスを除外します。

- 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
  untrust ポートで，信頼されていない DHCP サーバからの DHCP パケットを受信した場合，該当する DHCP パケットを廃棄します。これによって，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。

- 信頼されていない DHCP クライアントからの IP アドレス解放を抑止
  untrust ポートで，バインディングデータベース未登録の端末から IP アドレス解放要求を受信した場合，該当する DHCP パケットを廃棄します。これによって，DHCP サーバから IP アドレスを配布されていない端末からの IP アドレス解放を抑止します。
  また，同様に IP アドレス重複検出通知，リース時間更新，およびオプション情報取得要求を受信したときも DHCP パケットを廃棄します。これによって，信頼されていない DHCP クライアントからの不正な IP アドレスの解放，IP アドレスの取得，およびオプションの取得を抑止します。
- MAC アドレスの詐称を抑止
  untrust ポートで，受信した DHCP パケットの送信元 MAC アドレス（Source MAC Address）と，DHCP パケット内のクライアントハードウェアアドレス（chaddr）が不一致の場合，該当する DHCP パケットを廃棄します。これによって，MAC アドレスの詐称を抑止します。
- Option82 の詐称を抑止
  untrust ポートで，受信した DHCP パケットに Option82 が付与されている場合，該当する DHCP パケットを廃棄します。これによって，Option82 の詐称を抑止します。

13.1.3 DHCP パケットの受信レート制限

DHCP snooping 有効時に，受信する DHCP パケットを監視するとき，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 で設定します。本コマンドを設定していない場合は，受信レートを制限しません。

DHCP パケットの受信レート制限は，本装置が受信するすべての DHCP パケットを対象にします。

受信レートを超えた DHCP パケットは廃棄し，運用ログ情報を採取します。ただし，Trap は発行しません。なお，運用ログ情報は運用コマンド show ip dhcp snooping logging で確認できます。

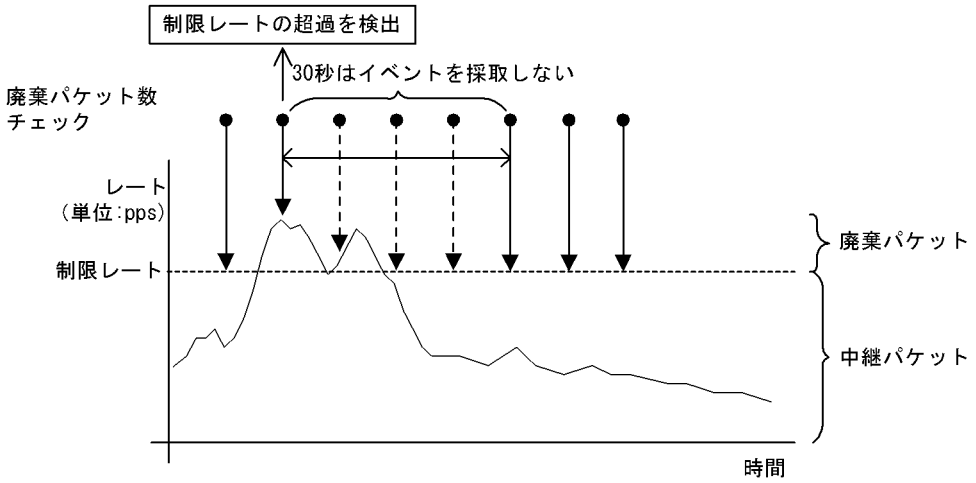
(1) 運用ログ情報の採取契機

運用ログ情報は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 30 秒間は，レート超過によってパケットを廃棄してもイベントを採取しません。

DHCP パケット受信レートの運用ログ情報の採取契機を次の図に示します。

図 13-6　DHCP パケット受信レートの運用ログ情報の採取契機



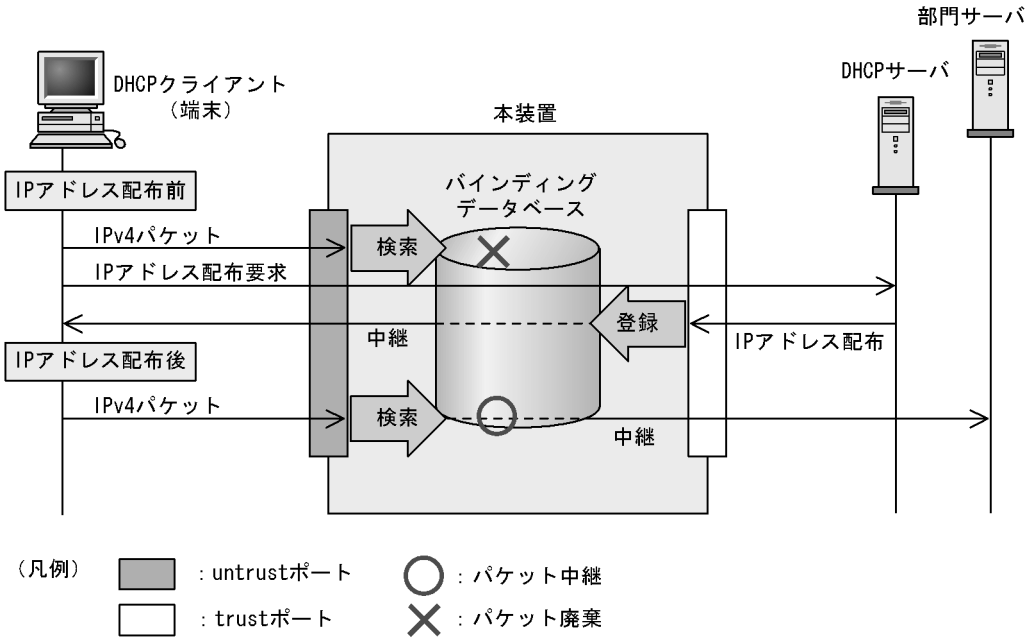
13.1.4　端末フィルタ

(1) 概要

端末フィルタは，本装置を通過する IPv4 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。

端末フィルタの動作概要を次の図に示します。

図 13-7　端末フィルタの動作概要



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できます。

なお，端末フィルタを使用する場合は，事前に受信側フロー検出モードに，端末フィルタの対応モード（layer2-dhcp-1）を設定する必要があります。

(2) IPv4 パケットの検査

untrust ポートで IPv4 パケットを受信した場合，バインディングデータベースとの整合性を検査し，未登録の端末であれば，該当する IPv4 パケットを廃棄します。

端末フィルタの検査対象を次の表に示します。

表 13-3 端末フィルタの検査対象

端末フィルタ条件	IPv4 パケット			
	受信インタフェース		Ethernet ヘッダ	IP ヘッダ
	ポート	VLAN ID	送信元 MAC アドレス	送信元 IP アドレス
送信元 MAC アドレスだけ	○	○	○	－
送信元 IP アドレスだけ	○	○	－	○
送信元 MAC アドレスと送信元 IP アドレス	○	○	○	○

（凡例）○：検査対象　－：検査対象外

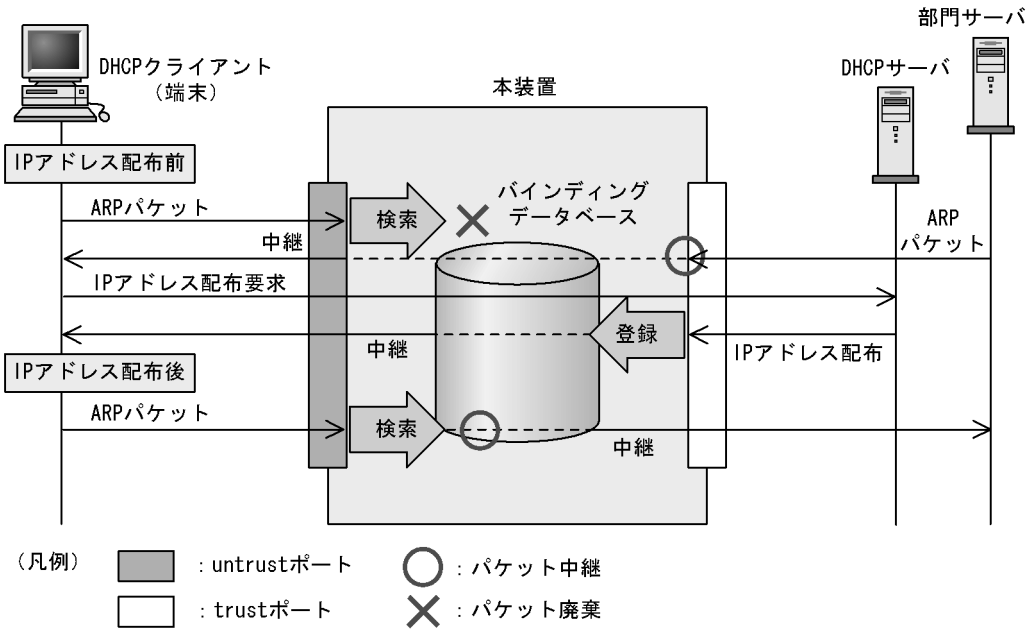
13.1.5 ダイナミック ARP 検査

(1) 概要

ダイナミック ARP 検査は，本装置を通過する ARP パケットを監視して，信頼されていない端末からの ARP パケットのアクセスを制限する機能です。

ダイナミック ARP 検査の動作概要を次の図に示します。

図 13-8　ダイナミック ARP 検査の動作概要



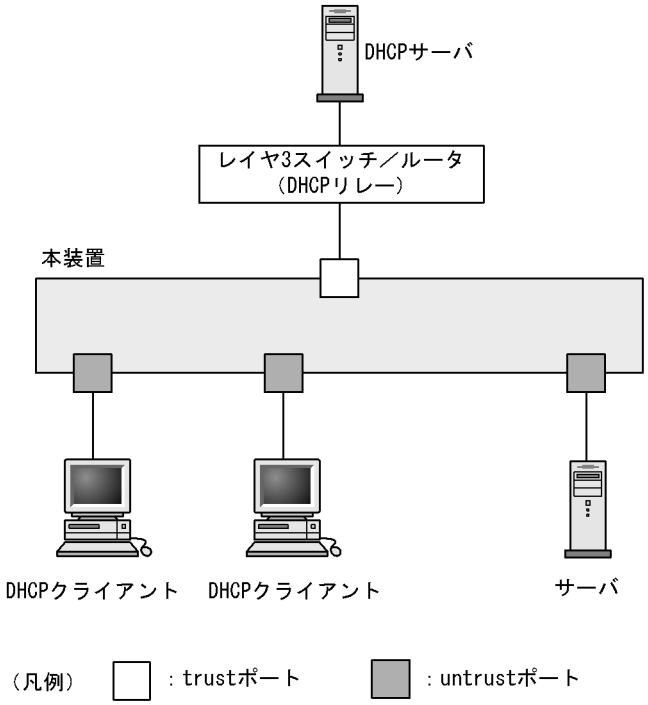
(2) ポートの種別

ダイナミック ARP 検査では DHCP snooping と同様に，ポートを次の種別に分類して，ARP パケットを監視します。

- trust ポート
  DHCP サーバや部門サーバなど，信頼済みの端末を接続するポートを trust ポートと呼びます。
  trust ポートで受信した ARP パケットは監視しません。
- untrust ポート
  DHCP クライアントなど，信頼されていない端末を接続するポートを untrust ポートと呼びます。
  DHCP サーバは接続しません。

ポートの種別を次の図に示します。

図 13-9 ポートの種別



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，デフォルトですべてのポートが untrust ポートになります。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 arp inspection trust で設定できます。

なお，ダイナミック ARP 検査では，コンフィグレーションコマンド ip arp inspection vlan で指定した VLAN を監視対象にします。

通常の運用では，コンフィグレーションコマンド ip dhcp snooping trust および ip arp inspection trust で指定するポートを一致させることをお勧めします。

(3) ARP パケットの基本検査

untrust ポートで，ARP パケットを受信した場合，バインディングデータベースとの整合性を検査し，未登録の端末であれば，該当する ARP パケットを廃棄します。

基本検査の検査対象を次の表に示します。

表 13-4 基本検査の検査対象

ARP 種別	受信インタフェース		ARP パケット					
	ポート	VLAN ID	Ethernet ヘッダ		ARP ヘッダ			
			宛先 MAC アドレス	送信元 MAC アドレス	送信元 MAC アドレス	送信元 IP アドレス	宛先 MAC アドレス	宛先 IP アドレス
Request	○	○	－	－	○	○	－	－
Reply	○	○	－	－	○	○	－	－

（凡例）○：検査対象　－：検査対象外

(4) ARP パケットのオプション検査

untrust ポートで，受信した ARP パケット内のデータの整合性を検査します。

オプション検査は，コンフィグレーションコマンド ip arp inspection validate で設定します。

(a) 送信元 MAC アドレス検査（src-mac 検査）

レイヤ 2 ヘッダに含まれる送信元 MAC アドレス（Source MAC）と，ARP ヘッダに含まれる送信元 MAC アドレス（Sender MAC Address）が同一であることを検査します。

ARP Request および ARP Reply の両方に対して検査します。

送信元 MAC アドレス検査の検査対象を次の表に示します。

表 13-5 送信元 MAC アドレス検査の検査対象

ARP 種別	受信インタフェース		ARP パケット					
	ポート	VLAN ID	Ethernet ヘッダ		ARP ヘッダ			
			宛先 MAC アドレス	送信元 MAC アドレス	送信元 MAC アドレス	送信元 IP アドレス	宛先 MAC アドレス	宛先 IP アドレス
Request	―	―	―	○	○	―	―	―
Reply	―	―	―	○	○	―	―	―

（凡例）○：検査対象　―：検査対象外

(b) 宛先 MAC アドレス検査（dst-mac 検査）

レイヤ 2 ヘッダに含まれる宛先 MAC アドレス（Destination MAC）と，ARP ヘッダに含まれる宛先 MAC アドレス（Target MAC Address）が同一であることを検査します。

ARP Reply に対してだけ検査します。

宛先 MAC アドレス検査の検査対象を次の表に示します。

表 13-6 宛先 MAC アドレス検査の検査対象

ARP 種別	受信インタフェース		ARP パケット					
	ポート	VLAN ID	Ethernet ヘッダ		ARP ヘッダ			
			宛先 MAC アドレス	送信元 MAC アドレス	送信元 MAC アドレス	送信元 IP アドレス	宛先 MAC アドレス	宛先 IP アドレス
Request	―	―	―	―	―	―	―	―
Reply	―	―	○	―	―	―	○	―

（凡例）○：検査対象　―：検査対象外

(c) IP アドレス検査（ip 検査）

ARP ヘッダに含まれる宛先 IP アドレス（Target IP Address）が次に示す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 に対してだけ検査します。

IP アドレス検査の検査対象を次の表に示します。

表 13-7 IP アドレス検査の検査対象

ARP 種別	受信インタフェース		ARP パケット					
	ポート	VLAN ID	Ethernet ヘッダ		ARP ヘッダ			
			宛先 MAC アドレス	送信元 MAC アドレス	送信元 MAC アドレス	送信元 IP アドレス	宛先 MAC アドレス	宛先 IP アドレス
Request	―	―	―	―	―	―	―	―
Reply	―	―	―	―	―	―	―	○

（凡例）○：検査対象　―：検査対象外

13.1.6 ARP パケットの受信レート制限

ダイナミック ARP 検査有効時に，受信する ARP パケットを監視するとき，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。本コマンドを設定していない場合は，受信レートを制限しません。

ARP パケットの受信レート制限は，本装置が受信するすべての ARP パケットを対象にします。

受信レートを超えた ARP パケットは廃棄し，運用ログ情報を採取します。ただし，Trap は発行しません。なお，運用ログ情報は運用コマンド show ip dhcp snooping logging で確認できます。

(1) 運用ログ情報の採取契機

運用ログ情報の採取契機は，DHCP パケットの受信レート制限と同様です。

採取契機については，「13.1.3　DHCP パケットの受信レート制限　(1) 運用ログ情報の採取契機」を参照してください。

13.1.7 DHCP snooping 使用時の注意事項

(1) VLAN 拡張機能のポート間中継遮断機能との共存

「コンフィグレーションガイド Vol.1　16.3 レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2) QoS との共存

端末フィルタと QoS（受信側）は，同一ポート内で共存できません。

(3) レイヤ 2 認証との共存

(a) Web 認証との共存

「5.2.1 レイヤ 2 認証と他機能との共存」を参照してください。

(b) 認証専用 IPv4 アクセスリスト設定時の注意

DHCP snooping と認証専用 IPv4 アクセスリストが共存する場合，認証専用 IPv4 アクセスリストのフィルタ条件にプロトコル名称 bootps または bootpc のどちらか一方を設定しても，そのほかのフィルタ条件に関係なく，bootps および bootpc の両方のパケットを透過します。

(c) ポートミラーリングとの共存

DHCP snooping を有効にした場合，本装置が送信するすべての DHCP パケットはミラーリングされません。また，ダイナミック ARP 検査も有効にした場合，本装置が送信するすべての ARP パケットもミラーリングされません。

(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 が設定されていない（初期状態）場合，バインディングデータベースは保存されません。装置を停止または再起動すると登録済のバインディングデータベースは消去されるため，DHCP クライアントからは通信できなくなります。通信できなくなった場合は，DHCP クライアント側で IP アドレスを解放および更新してください。例えば，Windows の場合，コマンドプロンプトから ipconfig /release を実行したあとに，ipconfig /renew を実行します。
  これによって，バインディングデータベースに端末情報が再登録され，DHCP クライアントから通信できるようになります。
- 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あと，装置の停止前または再起動前に時刻の設定を変更すると，装置の起動後にバインディングデータベースが正しく復元されないことがあります。
- コンフィグレーションコマンド ip source binding でスタティック登録したエントリは，スタートアップコンフィグレーションに従って復元されます。
- 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，装置の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。

(5) DHCP パケットの受信レート制限について

- DHCP パケットの受信レート制限および ARP パケットの受信レート制限が共存する場合，DHCP パケットと ARP パケットの受信レートを合計した値で監視します。

(6) ダイナミック ARP 検査について

- ダイナミック ARP 検査は，次に示すコンフィグレーションを設定して，バインディングデータベースが生成されていることが必要です。
  - ip dhcp snooping
  - ip dhcp snooping vlan
- 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。

(7) ARP パケットの受信レート制限について

- ARP パケットの受信レート制限および DHCP パケットの受信レート制限が共存する場合，ARP パケットと DHCP パケットの受信レートを合計した値で監視します。

13.2 コンフィグレーション

13.2.1 コンフィグレーションコマンド一覧

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 13-8 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	本装置の ARP パケットの受信レートを設定します。
ip arp inspection trust	ダイナミック ARP 検査で信頼済みの端末を接続するポートを設定します。
ip arp inspection validate	ダイナミック ARP 検査のオプション検査を設定します。
ip arp inspection vlan	ダイナミック ARP 検査を使用する VLAN を設定します。
ip dhcp snooping	DHCP snooping を有効に設定します。
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待ち時間を設定します。
ip dhcp snooping information option allow-untrusted	DHCP パケットの Option82 の詐称検査を無効に設定します。
ip dhcp snooping limit rate	本装置の DHCP パケットの受信レート制限を設定します。
ip dhcp snooping logging enable	動作ログの syslog サーバへの出力を設定します。
ip dhcp snooping loglevel	動作ログメッセージで記録するメッセージレベルを指定します。
ip dhcp snooping trust	DHCP snooping で信頼済みの端末を接続するポートを設定します。
ip dhcp snooping verify mac-address	DHCP パケットの MAC アドレスの詐称検査を無効に設定します。
ip dhcp snooping vlan	DHCP snooping を使用する VLAN を設定します。
ip source binding	固定 IP アドレスを持つ端末をバインディングデータベースに登録します。
ip verify source	端末フィルタを使用するポートを設定します。

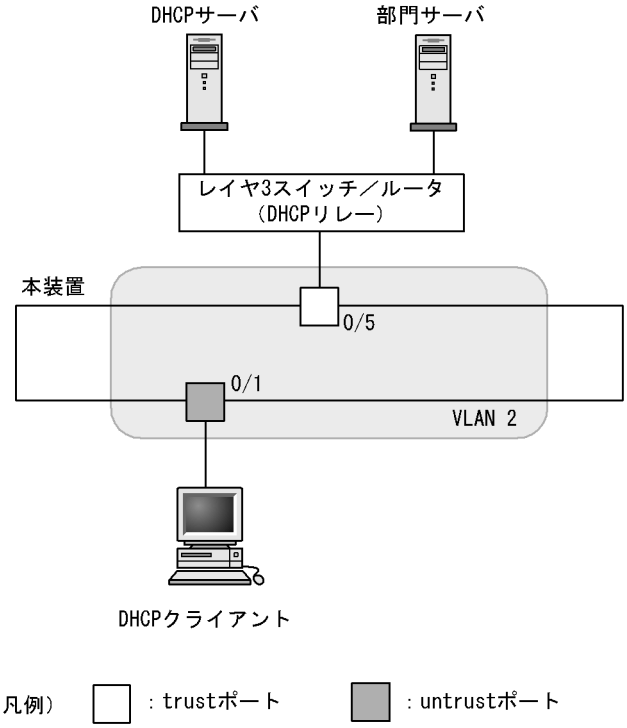
13.2.2 基本設定

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。

なお，DHCP snooping を使用する場合は，事前にコンフィグレーションコマンド flow detection mode で，DHCP snooping に対応する受信側フロー検出モードを設定しておく必要があります。

DHCP snooping の基本的な構成例を次の図に示します。

図 13-10 DHCP snooping の基本的な構成例



（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，さらに DHCP snooping を有効にする VLAN を設定します。

［コマンドによる設定］

1. **(config)# ip dhcp snooping**
   装置としての DHCP snooping 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 gigabitethernet 0/1**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 2
   (config-if)# 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） DHCP snooping の 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（「図 13-10　DHCP snooping の基本的な構成例」ではレイヤ 3 スイッチ／ルータと接続するポート）を trust ポートとして設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 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。そのほかのポートは 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) バインディングデータベースの保存先の設定

(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。

(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，および保存するファイル名として 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 はアラクサラ製品をご使用ください。

(4) バインディングデータベースの保存先への書き込み待ち時間の設定

[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待ち時間を設定します。

[コマンドによる設定]

1. **(config)# ip dhcp snooping database write-delay 3600**
   次のどれかを保存契機として，保存を開始するまでの時間を 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，および削除時
   - 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。

13.2.3 DHCP パケットの受信レート制限

DHCP パケットの受信レート制限を使用するための設定について説明します。

[設定のポイント]

本装置が端末から受信する DHCP パケットの受信レートを設定します。

[コマンドによる設定]

1. **(config)# ip dhcp snooping limit rate 50**
   本装置の受信レートを 50 パケット / 秒に設定します。

13.2.4 端末フィルタ

端末フィルタを使用するための設定について説明します。

[設定のポイント]

DHCP クライアントを接続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 gigabitethernet 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 アドレスを端末フィルタ条件とする端末フィルタを設定します。

[注意事項]

trust ポートでコンフィグレーションコマンド ip verify source 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，コンフィグレーションコマンド 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注意してください。

13.2.5 ダイナミック ARP 検査

ダイナミック ARP 検査を使用するための設定について説明します。

(1) 基本設定

[設定のポイント]

ダイナミック ARP 検査の基本検査を有効にする VLAN を設定します。

[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 検査の対象に設定します。本コマンドを指定しない VLAN ではダイナミック ARP 検査は動作しません。

[注意事項]

- 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。
- 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のエントリも，ダイナミック ARP 検査の対象となります。
- 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，そのポートはダイナミック ARP 検査の対象外となります。

(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を trust ポートとして設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/5**
   (config-if)# ip arp inspection trust
   (config-if)# exit
   ポート 0/5 を trust ポートとして設定します。そのほかのポートは untrust ポートとなります。

[注意事項]

本コマンドを設定したポートでは，ダイナミック ARP 検査の検査対象 VLAN に所属していても，ダイナミック ARP 検査の対象外となります。

(3) オプション検査の設定

[設定のポイント]

本装置のダイナミック ARP 検査のオプション検査として送信元 MAC アドレス検査（src-mac 検査）を有効に設定します。

[コマンドによる設定]

1. **(config)# ip arp inspection validate src-mac**
   オプション検査として送信元 MAC アドレス検査（src-mac 検査）を有効に設定します。

13.2.6 ARP パケットの受信レート制限

ARP パケットの受信レート制限を使用するための設定について説明します。

[設定のポイント]

本装置が受信する ARP パケットの受信レートを設定します。

[コマンドによる設定]

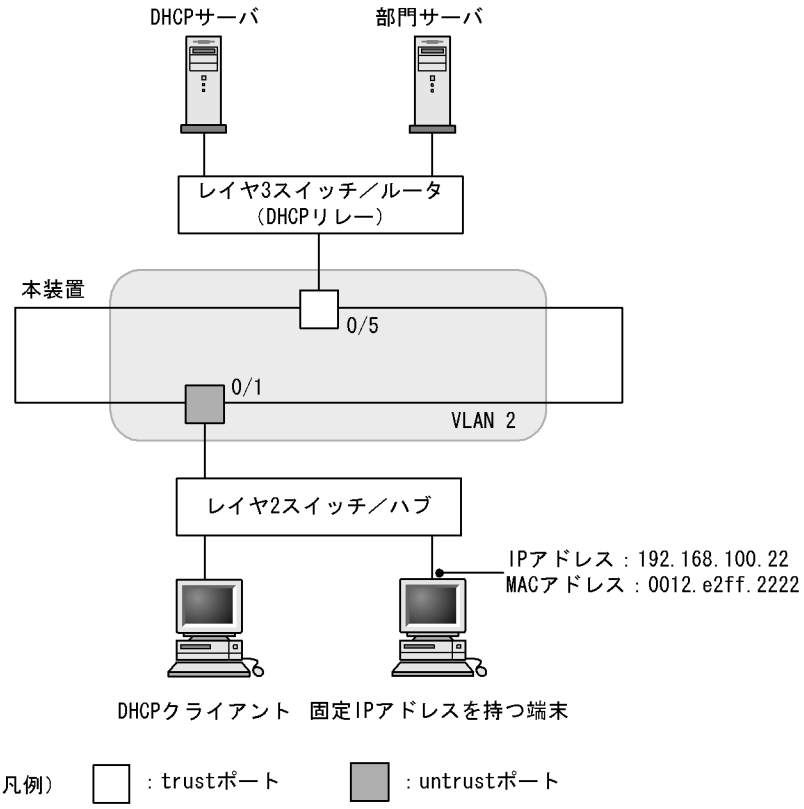
1. **(config) # ip arp inspection limit rate 100**
   本装置の受信レートを 100 パケット / 秒に設定します。

13.2.7 固定 IP アドレスを持つ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。

固定 IP アドレスを持つ端末を接続した場合の構成例を次の図に示します。

図 13-11　固定 IP アドレスを持つ端末を接続した場合の構成例



DHCP snooping の設定は，「13.2.2　基本設定」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 アドレスを持つ端末のスタティック登録が必要です。

［設定のポイント］

固定 IP アドレスを持つ端末の端末情報を，バインディングデータベースにスタティック登録します。

［コマンドによる設定］

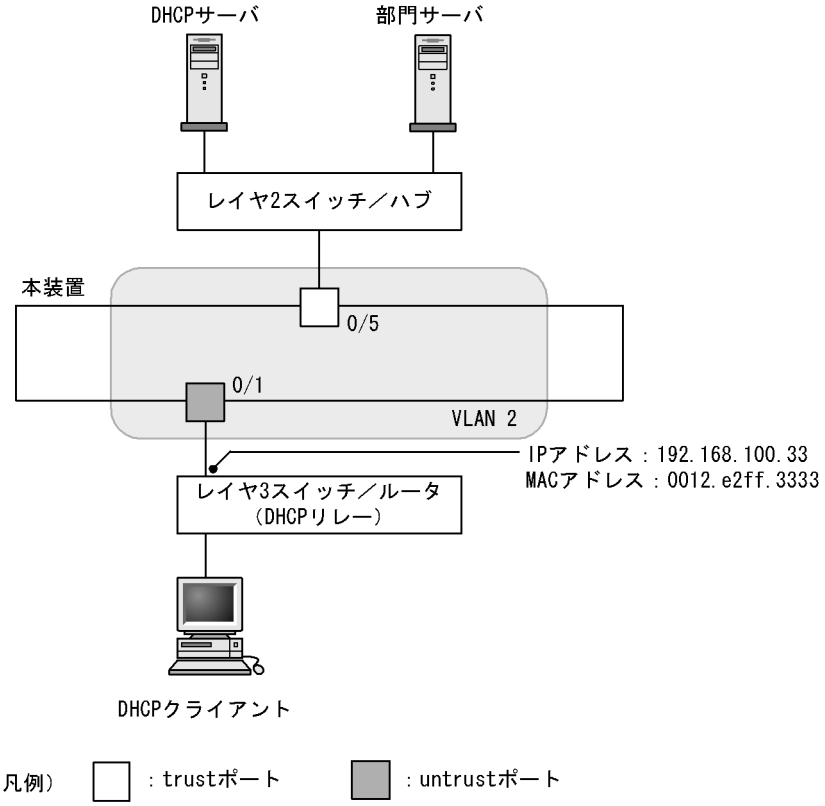
1. **(config)# ip source binding 0012.e2ff.2222 vlan 2 192.168.100.22 interface gigabitethernet 0/1**
   端末の MAC アドレス，端末が所属する VLAN（VLAN ID），端末の IP アドレス，および端末が接続されているポート番号を，バインディングデータベースに設定します。

13.2.8　本装置の配下に DHCP リレーが接続された場合

本装置の配下に DHCP リレーを接続した場合，本装置でパケットを中継できるように設定します。

本装置の配下に DHCP リレーを接続した場合の構成例を次の図に示します。

図 13-12　本装置の配下に DHCP リレーを接続した場合の構成例



本装置の DHCP snooping 設定は，「13.2.2　基本設定」，「13.2.4　端末フィルタ」，および「13.2.5　ダイナミック ARP 検査」と同様です。

本例では，そのままでは DHCP クライアントからの DHCP パケットおよび IPv4 パケットが中継できません。また，レイヤ 3 スイッチ／ルータからの ARP パケットも中継できません。

パケットを中継するためには，本装置で DHCP パケットの中継を許可する設定，IPv4 パケットの中継を許可する設定，および ARP パケットの中継を許可する設定が必要です。

（1） DHCP パケットの中継を許可する設定

［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／ルータ（DHCP リレー）によって送信元 MAC アドレスが書き換えられているため，DHCP パケットの MAC アドレス詐称検査を無効に設定します。

［コマンドによる設定］

1. **(config)# no ip dhcp snooping verify mac-address**
   untrust ポートの MAC アドレス詐称検査を無効に設定します。

［注意事項］

本コマンドが設定されていない場合，MAC アドレス詐称検査をするため，untrust ポートに DHCP リレーを接続できません。

(2) IPv4 パケットの中継を許可する設定

[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／ルータ（DHCP リレー）によって送信元 MAC アドレスが書き換えられているため，端末フィルタ条件に送信元 IP アドレスだけを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# ip verify source
   (config-if)# exit
   ポート 0/1 に，端末フィルタ条件として送信元 IP アドレスだけを設定します。

(3) ARP パケットの中継を許可する設定

ARP パケットの中継を許可する設定は固定 IP アドレスを持つ端末を接続した場合と同様です。

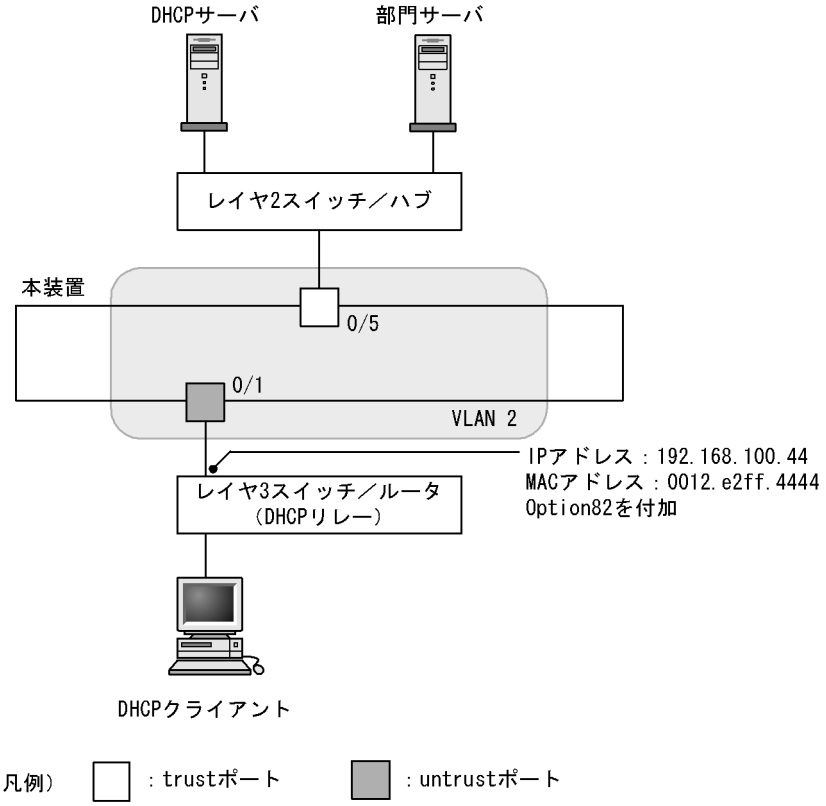
設定については，「13.2.7　固定 IP アドレスを持つ端末を接続した場合」を参照してください。

13.2.9　本装置の配下に Option82 を付与する DHCP リレーが接続された場合

本装置の配下に Option82 を付与する DHCP リレーを接続した場合，本装置でパケットを中継できるように設定します。

本装置の配下に Option82 を付与する DHCP リレーを接続した場合の構成例を次の図に示します。

図 13-13　本装置の配下に Option82 を付与する DHCP リレーを接続した場合の構成例



本装置の DHCP snooping 設定は「13.2.2　基本設定」,「13.2.4　端末フィルタ」, および「13.2.5　ダイナミック ARP 検査」と同様です。

本例では，そのままでは DHCP クライアントからの DHCP パケットおよび IPv4 パケットが中継できません。また，レイヤ 3 スイッチ／ルータからの ARP パケットも中継できません。

パケットを中継するためには，本装置で DHCP パケットの中継を許可する設定，IPv4 パケットの中継を許可する設定，および ARP パケットの中継を許可する設定が必要です。また，DHCP リレーが Option82 を付与する場合，Option82 付き DHCP パケットの中継を許可する設定も必要です。

(1) DHCP パケットの中継を許可する設定

DHCP パケットの中継を許可する設定は本装置の配下に DHCP リレーが接続された場合と同様です。

設定については,「13.2.8　本装置の配下に DHCP リレーが接続された場合　(1) DHCP パケットの中継を許可する設定」を参照してください。

(2) IPv4 パケットの中継を許可する設定

DHCP パケットの中継を許可する設定は本装置の配下に DHCP リレーが接続された場合と同様です。

設定については,「13.2.8　本装置の配下に DHCP リレーが接続された場合　(2) IPv4 パケットの中継を許可する設定」を参照してください。

(3) ARP パケットの中継を許可する設定

ARP パケットの中継を許可する設定は固定 IP アドレスを持つ端末を接続した場合と同様です。

設定については，「13.2.7　固定 IP アドレスを持つ端末を接続した場合」を参照してください。

（4） Option82 付き DHCP パケットの中継を許可する設定

［設定のポイント］

DHCP パケットの Option82 の詐称検査を無効に設定します。

［コマンドによる設定］

1. **(config)# ip dhcp snooping information option allow-untrusted**
   untrust ポートの Option82 の詐称検査を無効に設定します。

13.2.10　syslog サーバへの出力

［設定のポイント］

動作ログを syslog サーバに出力する設定をします。

［コマンドによる設定］

1. **(config)# ip dhcp snooping logging enable**
   動作ログを syslog サーバに出力する設定をします。

2. **(config)# logging event-kind dsn**
   syslog サーバに送信対象とするログ情報の，イベント種別に DHCP snooping を設定します。

13.3 オペレーション

13.3.1 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 13-9 運用コマンド一覧

コマンド名	説明
show ip dhcp snooping binding	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	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	統計情報を表示します。
clear ip dhcp snooping statistics	統計情報をクリアします。
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 logging	プログラムで採取しているログメッセージを表示します。
clear ip dhcp snooping logging	プログラムで採取しているログメッセージをクリアします。
restart dhcp snooping	プログラムを再起動します。
dump protocols dhcp snooping	プログラムで採取しているログや内部情報をファイルへ出力します。

13.3.2 DHCP snooping 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 show ip dhcp snooping binding コマンドで表示します。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。

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

図 13-14 show ip dhcp snooping binding の実行結果

```
> show ip dhcp snooping binding
Date 2010/04/20 12:00:00 UTC
Agent URL: flash
Last succeeded time: 2010/04/20 11:50:00 UTC
Total Bindings Used/Max    :       5/   250
Total Source guard Used/Max:       2/   250

Bindings: 5
MAC Address     IP Address       Expire(min)  Type      VLAN  Port
0012.e287.0001  192.168.0.201    -            static*   1     0/1
0012.e287.0002  192.168.0.204    1439         dynamic   2     0/4
0012.e287.0003  192.168.0.203    -            static    3     0/3
0012.e287.0004  192.168.0.202    3666         dynamic   4     ChGr:2
0012.e2be.b0fb  192.168.100.11   59           dynamic*  12    0/11
>
```

13.3.3 DHCP snooping 統計情報の確認

DHCP snooping 統計情報を show ip dhcp snooping statistics コマンドで表示します。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，およびフィルタした DHCP パケット数を表示します。

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

図 13-15 show ip dhcp snooping statistics の実行結果

```
> show ip dhcp snooping statistics
Date 2010/04/20 12:00:00 UTC
Database Exceeded: 0
Total DHCP Packets: 8995
Port            Recv      Filter
0/1              170         170
0/3             1789          10
             :
0/25               0           0
ChGr:1          3646        2457
>
```

13.3.4 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 show ip arp inspection statistics コマンドで表示します。中継した ARP パケット数，廃棄した ARP パケット数，および廃棄 ARP パケット数の内訳を表示します。

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

図 13-16 show ip arp inspection statistics の実行結果

```
> show ip arp inspection statistics
Date 2010/04/20 12:00:00 UTC
Port       Forwarded     Dropped  ( DB mismatch     Invalid  )
0/1                0          15  (           15           0  )
0/2              584         883  (          883           0  )
0/3                0           0  (            0           0  )
                               :
ChGr:2           170          53  (           53           0  )
>
```

13.3.5 DHCP snooping ログメッセージの確認

DHCP snooping ログメッセージを show ip dhcp snooping logging コマンドで表示します。バインディングデータベースの更新，端末フィルタの更新，不正な DHCP サーバの検出，不正な DHCP パケットの廃棄，または ARP パケットの廃棄などのログメッセージを表示します。

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

図 13-17 show ip dhcp snooping logging の実行結果

```
> show ip dhcp snooping logging
Date 2010/04/20 12:00:00 UTC
Apr 20 11:00:00 ID=2201 NOTICE DHCP server packets were received at an untrust
port(0/2/1/0012.e2ff.fe01/192.168.100.254).
>
```

14 GSRP の解説

GSRP は，装置の冗長化を行う機能です。この章では，GSRP の概要について説明します。

14.1　GSRP の概要

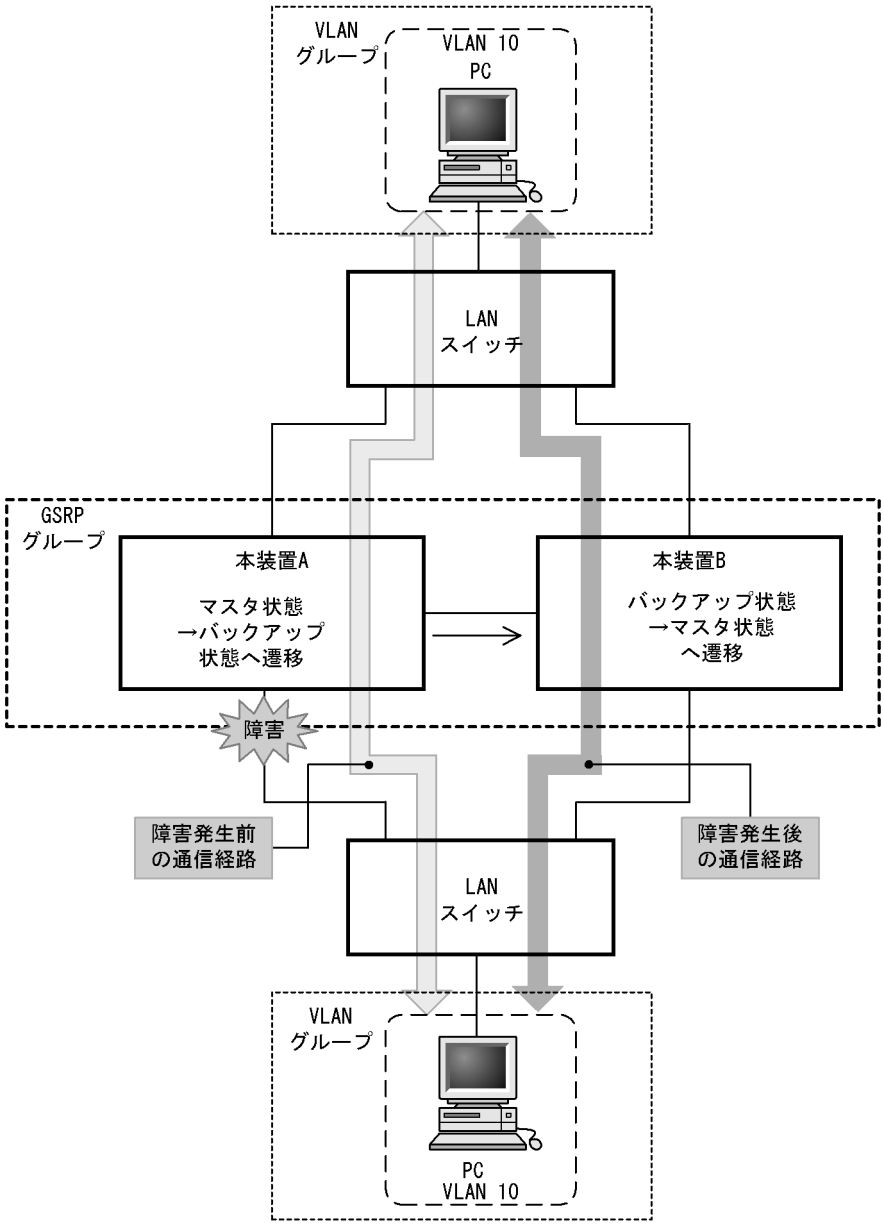
14.1.1　概要

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

ネットワークの冗長化を行う機能としてスパニングツリーがありますが，GSRP では 2 台のスイッチ間で制御するため，スパニングツリーよりも装置間の切り替えが高速です。また，ネットワークのコアスイッチを多段にするような大規模な構成にも適しています。一方で，スパニングツリーは標準プロトコルであり，マルチベンダーによるネットワーク構築に適しています。

GSRP によるレイヤ 2 の冗長化の概要を次の図に示します。

図 14-1　GSRP の概要



GSRP 機能を動作させる本装置 2 台をペアにしてグループを構成し，通常運用では片側をマスタ状態，もう一方をバックアップ状態として稼働させます。マスタ状態の本装置 A はフレームをフォワーディングし，バックアップ状態の本装置 B はブロッキングします。リンクの障害や装置障害などが発生した場合，本装置 A，B 間でマスタ状態とバックアップ状態の切り替えを行います。これによって，通信を継続できます。

14.1.2 特長

(1) 同時マスタ状態の回避

GSRP では本装置間を直接接続するリンク上で状態確認用の制御フレームの送受信を行い，対向装置の状態を確認します。制御フレームの送受信が正常にできている間にリンクの障害などを検出した場合は，自動的に切り替えを行います。その際，本装置は，対向の本装置が確実にバックアップ状態として稼働中であることを確認した上でマスタ状態へ切り替わります。これによって 2 台の本装置が同時にマスタ状態になることを回避します。

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

(2) 制御フレームの送信範囲の限定

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

14.1.3 サポート仕様

GSRP でサポートする項目と仕様を次の表に示します。

表 14-1 GSRP でサポートする項目・仕様

項目		内容
適用レイヤ	レイヤ 2	○
	レイヤ 3	×
装置当たりの GSRP グループ最大数		1
GSRP グループを構成する本装置の最大数		2
GSRP グループ当たりの VLAN グループ最大数		64
VLAN グループ当たりの VLAN 最大数		1024
GSRP Advertise フレーム送信間隔		0.5 ～ 60 秒の範囲で 0.5 秒単位
GSRP Advertise フレーム保有時間		1 ～ 120 秒の範囲で 1 秒単位
ロードバランス機能		○
バックアップ固定機能		○
ポートリセット機能		○
リンク不安定時の連続切り替え防止機能		○

項目	内容
GSRP VLAN グループ限定制御機能	○
GSRP 制御対象外ポート	○

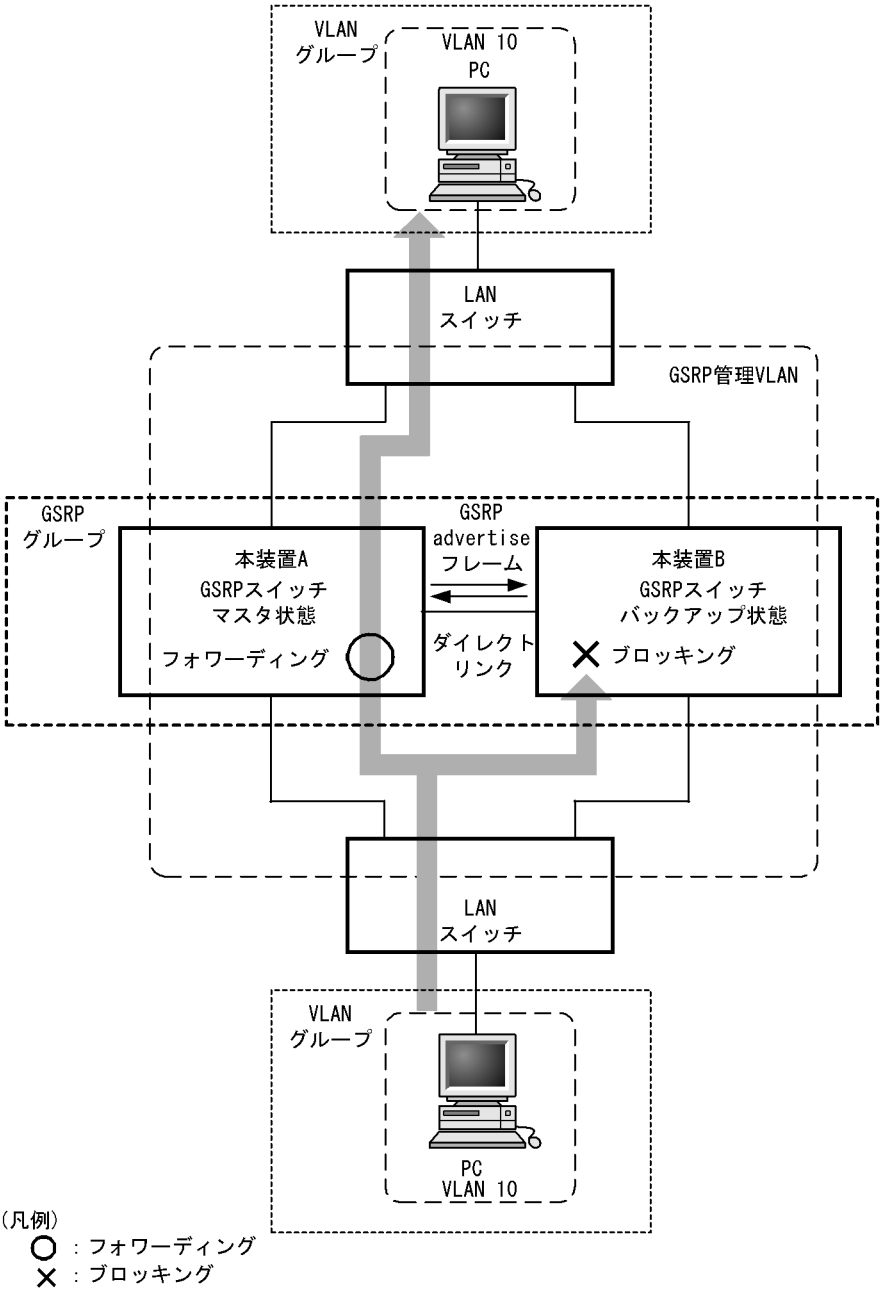
（凡例） ○：サポート　×：未サポート

14.2　GSRP の基本原理

14.2.1　ネットワーク構成

GSRP を使用する場合の基本的なネットワーク構成を次の図に示します。

図 14-2　GSRP のネットワーク構成



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

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

ダイレクトリンク上では GSRP Advertise フレームと呼ぶ状態確認用の制御フレームを送受信します。デフォルトの状態ではそのほかのデータフレームはブロッキングします。そのほかのデータフレームも送受信したい場合は，GSRP VLAN グループ限定制御機能を設定して，VLAN グループに所属しない VLAN を使用するか，ダイレクトリンクを GSRP 制御対象外ポートに設定します。

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

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

14.2.2 GSRP 管理 VLAN

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

GSRP スイッチはマスタ状態へ遷移する際，周囲のスイッチに向けて MAC アドレステーブルエントリのクリアを要求するため，GSRP Flush request フレームと呼ぶ制御フレームを送信します。このため，GSRP 管理 VLAN には，ダイレクトリンクのポートだけでなく VLAN グループに参加させるすべての VLAN のポートを設定する必要があります。また，周囲のスイッチでも GSRP の制御フレームを受信できるように，GSRP 管理 VLAN と同一の VLAN の設定をしておく必要があります。ただし，VLAN グループに参加させる VLAN のポートのうち，GSRP Flush request フレームの受信による MAC アドレステーブルのクリアをサポートしていないスイッチとの接続ポート，およびその対向のポートには，GSRP 管理 VLAN の設定をする必要はありません。

14.2.3 GSRP の切り替え制御

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

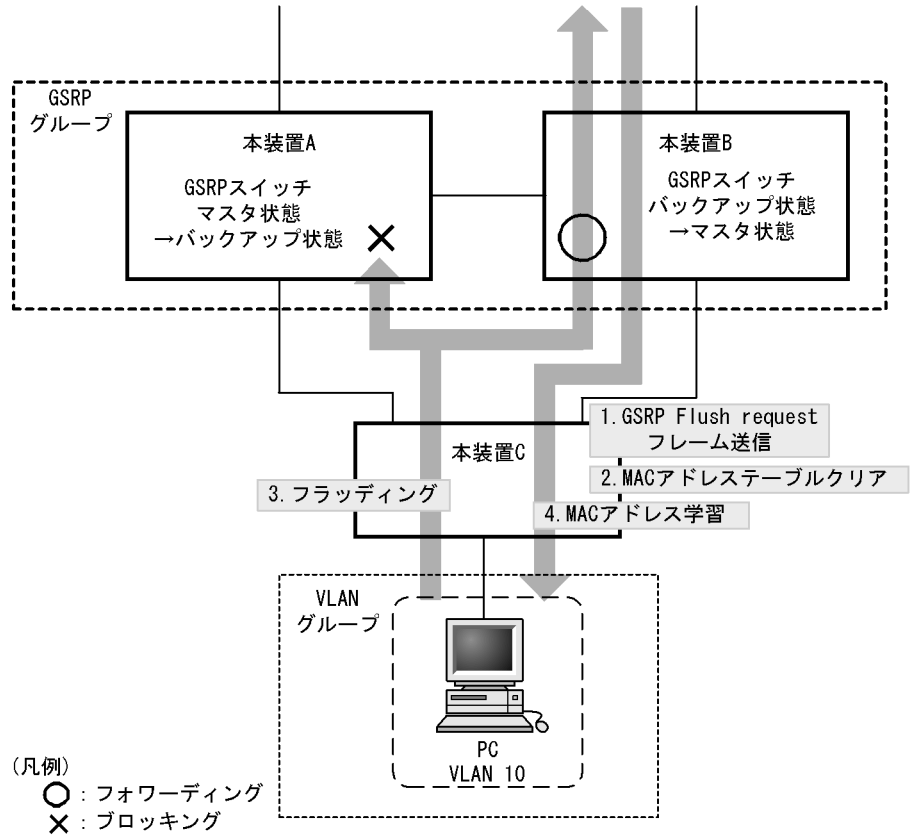
GSRP では，周囲のスイッチの MAC アドレステーブルエントリをクリアする方法として下記をサポートしています。

（1） GSRP Flush request フレームの送信

GSRP では切り替えを行うとき，周囲のスイッチに対して MAC アドレステーブルエントリのクリアを要求するため GSRP Flush request フレームと呼ぶ制御フレームを送信します。この GSRP Flush request フレームを受信して，自装置内の MAC アドレステーブルをクリアできるスイッチを GSRP aware と呼びます。本装置は特にコンフィグレーションの設定がないと，常に GSRP aware として動作します。GSRP aware は GSRP Flush request フレームをフラッディングします。一方，GSRP Flush Request フレームに対する機能をサポートしていないスイッチを GSRP unaware と呼びます。周囲のスイッチが GSRP unaware である場合は，「（2）ポートリセット機能」を使用する必要があります。GSRP Flush request フ

レームによる切り替え制御の概要を次の図に示します。

図 14-3 GSRP Flush request フレームによる切り替え制御の概要



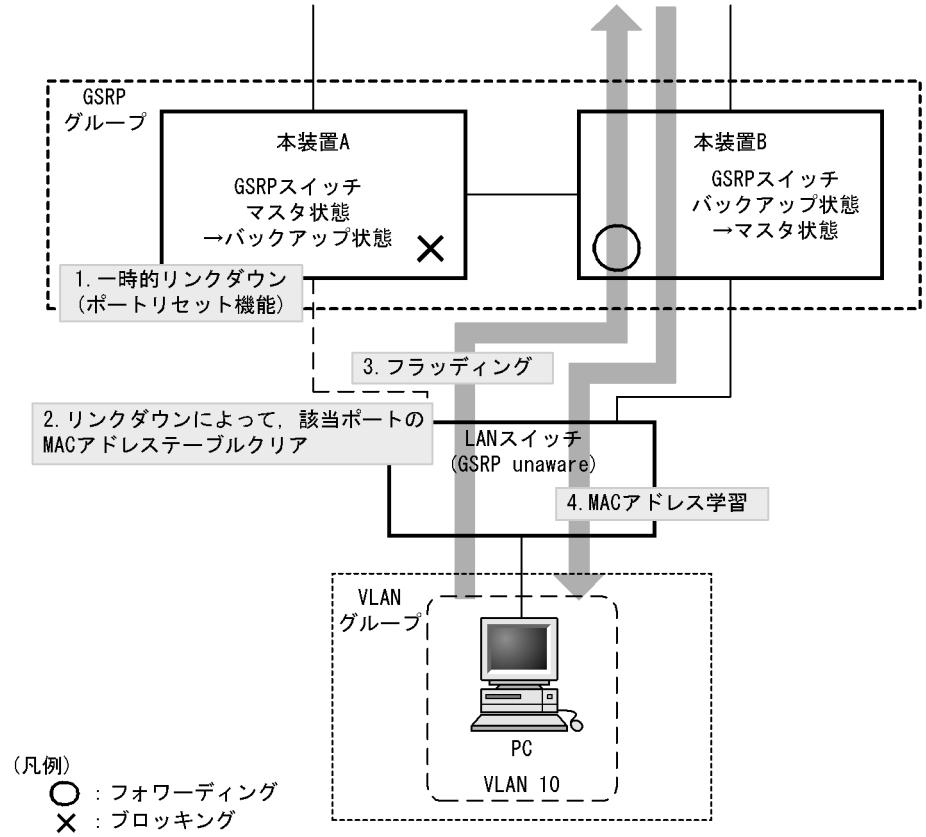
1. 本装置 A と本装置 B との間で切り替えが行われ，本装置 B は GSRP Flush request フレームを本装置 C へ向けて送信します。
2. 本装置 C は GSRP Flush request フレームを受けて，自装置内の MAC アドレステーブルをクリアします。
3. この結果，本装置 C 上は PC の送信するフレームに対して，MAC アドレスの学習が行われるまでフラッディングを行います。
   当該フレームは，マスタ状態である本装置 B を経由して宛先へフォワーディングされます。
4. 応答として PC 宛のフレームが戻ってくると，本装置 C は MAC アドレスの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

(2) ポートリセット機能

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

ポートリセット機能による切り替え制御の概要を次の図に示します。

図 14-4 ポートリセット機能による切り替え制御の概要



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

14.2.4 マスタ，バックアップの選択方法

(1) 選択基準

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

表 14-2 GSRP でサポートするマスタ，バックアップの選択基準

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

(2) 選択優先順

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

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

14.3 GSRP の動作概要

14.3.1 GSRP の状態

GSRP は五つの状態を持ち動作します。状態の一覧を次の表に示します。

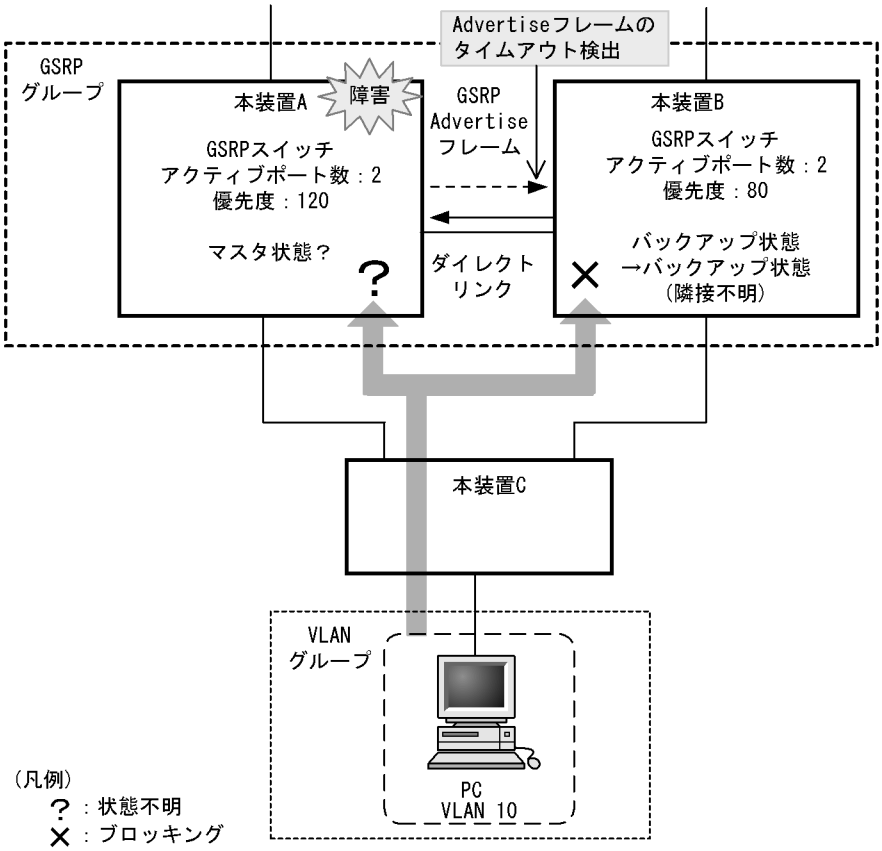
表 14-3 GSRP の状態一覧

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

14.3.2 装置障害時の動作

装置障害時の動作例を次の図に示します。

図 14-5 装置障害時の動作



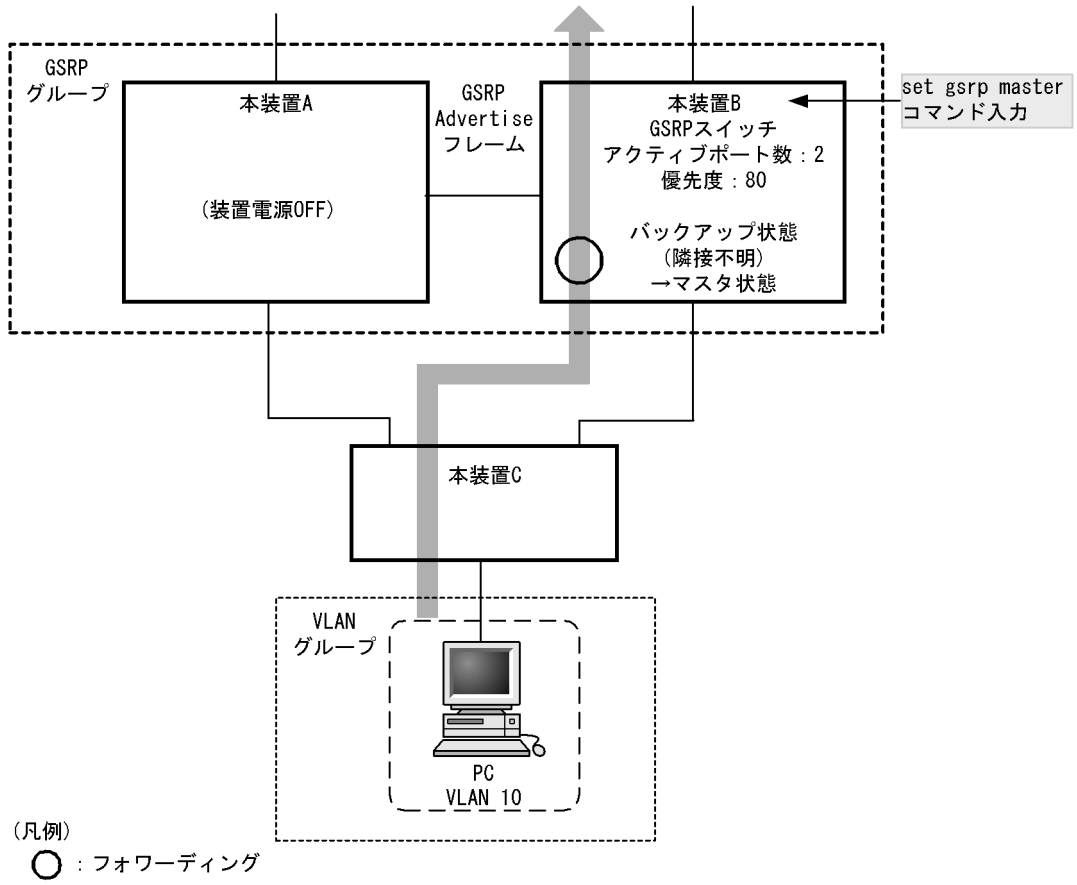
装置障害などが発生したことによって，マスタ状態の本装置 A が GSRP Advertise フレームを正常に送信できなくなった場合，本装置 B は本装置 A からの GSRP Advertise フレームの受信タイムアウトを検出します。このとき，本装置 B はバックアップ（隣接不明）状態に遷移します。バックアップ（隣接不明）状態では，バックアップ状態と同様，フレームの中継は行いません。バックアップ（隣接不明）状態になった場合，メッセージを出力し，運用者に対して装置の状態の確認を促します。

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

（1）手動による切り替え（運用コマンドによる切り替え）

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

図 14-6 運用コマンド set gsrp master 入力後の動作



(2) 自動での切り替え（ダイレクトリンク障害検出による切り替え）

自動での切り替えを行う機能として，ダイレクトリンク障害検出機能をサポートしています。また，ダイレクトリンク障害検出機能では対象外となる，装置起動時も自動で切り替えを行う GSRP スイッチ単独起動時のマスタ遷移機能もサポートしています。

- **ダイレクトリンク障害検出機能**
  ダイレクトリンク障害検出機能を動作させるには，コンフィグレーションコマンド no-neighbor-to-master でパラメータ direct-down を指定します。
  本機能は，装置起動後，対向装置からの GSRP Advertise フレームを受信したあとで有効になります。VLAN グループがバックアップ（隣接不明）状態に遷移した際，ダイレクトリンクのポートがダウン状態であれば，対向装置が装置障害状態であるとみなして，自動的にマスタ状態へ遷移します。
  装置起動時※1 から対向装置からの GSRP Advertise フレームを受信するまでは，対向装置の状態が不明のため，ダイレクトリンク障害検出機能による自動での切り替えは行いません。マスタとして動作させたい場合は，手動で切り替えてください。装置起動時など，対向装置からの GSRP Advertise フレームを受信していないときにも自動で切り替えたい場合は，GSRP スイッチ単独起動時のマスタ遷移機能を使用することによって，マスタへ遷移させることもできます。
- GSRP **スイッチ単独起動時のマスタ遷移機能**
  GSRP スイッチ単独起動時のマスタ遷移機能を動作させるには，コンフィグレーションコマンド no-neighbor-to-master でパラメータ direct-down forced-shift-time を指定します。
  本機能は，対向となる GSRP スイッチが障害などによって起動せず，装置起動時※2 からダイレクトリンクがアップしていない時にだけ動作します。

GSRP スイッチ単独起動時のマスタ遷移機能を開始する条件※3 をすべて満たすと自動マスタ遷移待ち状態になり，パラメータ forced-shift-time で設定する自動マスタ遷移待ち時間経過後に自動的にマスタ状態へ遷移します。
自動マスタ遷移待ち状態では，運用コマンド clear gsrp forced-shift によって，自動マスタ遷移待ち状態を解除して VLAN グループが自動的にマスタ遷移する動作を抑止できます。
本機能は，対向装置の状態が不明なままマスタに遷移させることになります。自動的にマスタとして動作するまでの時間は，対向装置のポートがブロッキングされていること，または装置が起動していないことを十分に保障できる時間を設定してください。

注※ 1

次の動作が行われたときも，装置起動時と同じ動作になります。

- 運用コマンド restart vlan の実行
- 運用コマンド restart gsrp の実行
- コンフィグレーションコマンド gsrp の no-neighbor-to-master で direct-down を指定
- コンフィグレーションコマンド gsrp の direct-link によるダイレクトリンクポートの設定
- 運用コマンド copy によるランニングコンフィグレーションへの反映

注※ 2

次の動作が行われたときも，装置起動時と同様に GSRP スイッチ単独起動時のマスタ遷移機能が動作します。

- 運用コマンド restart vlan の実行
- 運用コマンド restart gsrp の実行
- 運用コマンド copy によるランニングコンフィグレーションへの反映

注※ 3

GSRP スイッチ単独起動時のマスタ遷移機能を開始する条件を次に示します。

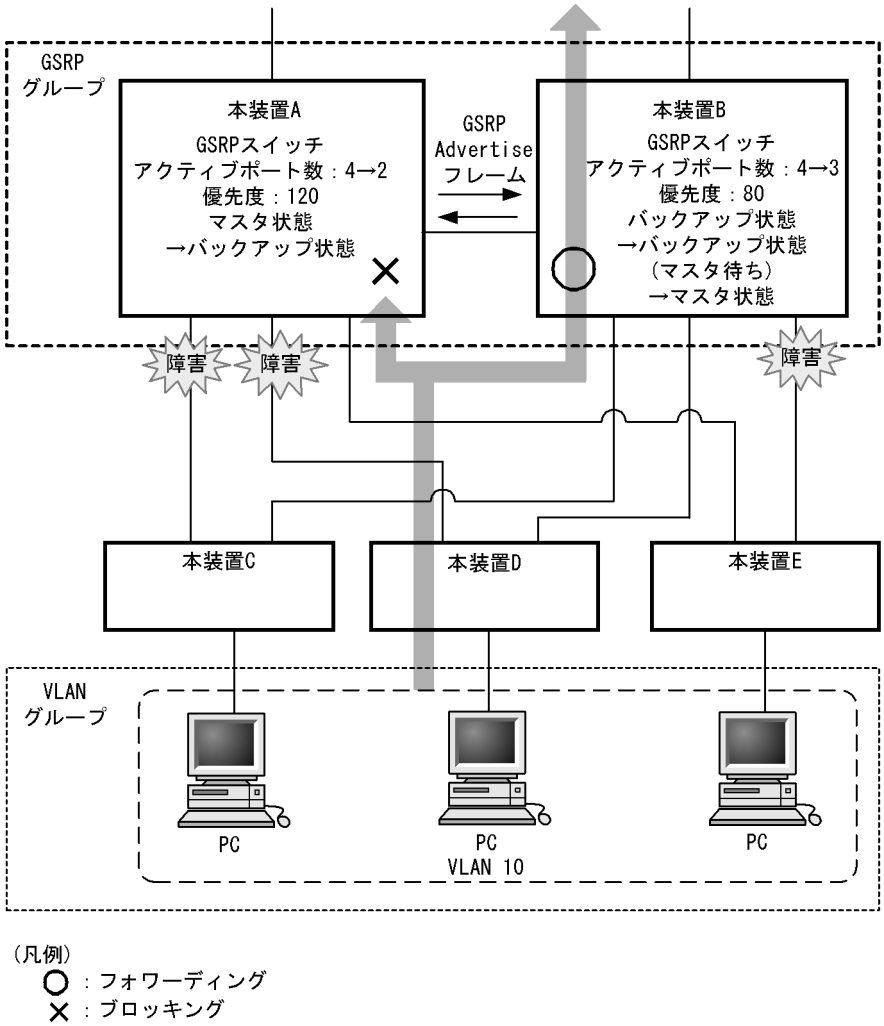
- GSRP Advertise フレームの受信タイムアウトが発生
- 本装置に設定されている VLAN グループのどれかのメンバポートがアップ

14.3.3 リンク障害時の動作

(1) リンク障害時の動作例

リンク障害時の動作例を次の図に示します。

図 14-7 リンク障害時の動作例



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

(2) リンク不安定時の連続切り替え防止機能

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

そのため，GSRP ではリンクが安定化したことを運用者が確認できるまでの間，アップしたリンクのポートをアクティブポート数としてカウントしないようにするための遅延時間をコンフィグレーションコマンド port-up-delay で設定できます。これによって，リンク不安定時の不用意な切り替えを抑止できます。

port-up-delay コマンドでは 1 から 43200 秒（12 時間）内で 1 秒単位に指定できます。また，infinity と設定することで，遅延時間を無限とすることもできます。リンクが安定したことを確認できた場合，port-up-delay コマンドで指定した遅延時間を待たないですぐにアクティブポート数としてカウントするための運用コマンド clear gsrp port-up-delay もサポートしています。

14.3.4 バックアップ固定機能

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

14.3.5 GSRP VLAN グループ限定制御機能

コンフィグレーションコマンド gsrp limit-control によって，GSRP の制御対象を VLAN グループに所属する VLAN に限定して運用できます。VLAN グループに所属しない VLAN は，GSRP の制御対象外になり，常時通信可能な VLAN となります。

14.3.6 GSRP 制御対象外ポート

コンフィグレーションコマンド gsrp exception-port によって，指定したポートを GSRP 制御対象外ポートとして運用できます。GSRP 制御対象外ポートにすることで，マスタ / バックアップ状態に関係なく，常時通信可能なポートとなります。

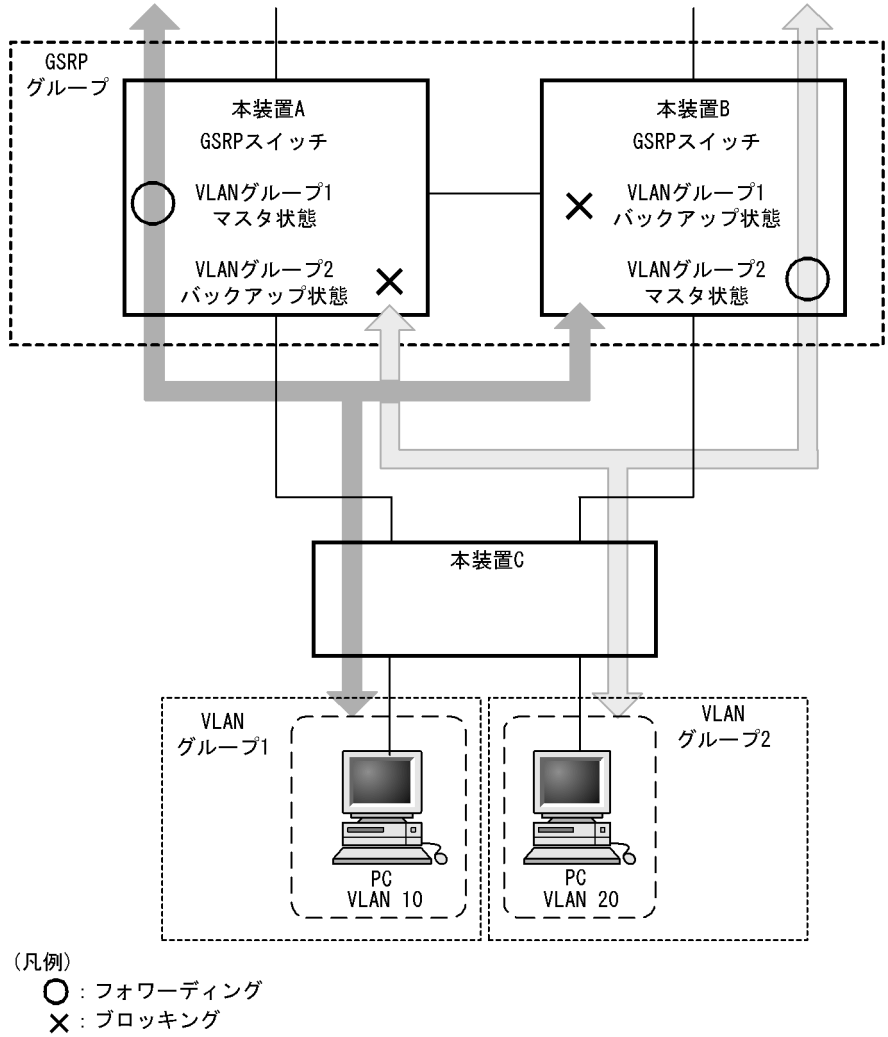
14.4　GSRP のネットワーク設計

14.4.1　VLAN グループ単位のロードバランス構成

GSRP では，VLAN グループ単位にマスタ状態，バックアップ状態の状態管理を行います。1 台の GSRP スイッチで最大 64 個の VLAN グループまで設定できます。複数の VLAN グループを同居させることで，VLAN グループ単位のロードバランス構成をとり，トラフィックの負荷分散を図ることができます。ロードバランス構成の概要を次の図に示します。

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

図 14-8　ロードバランス構成

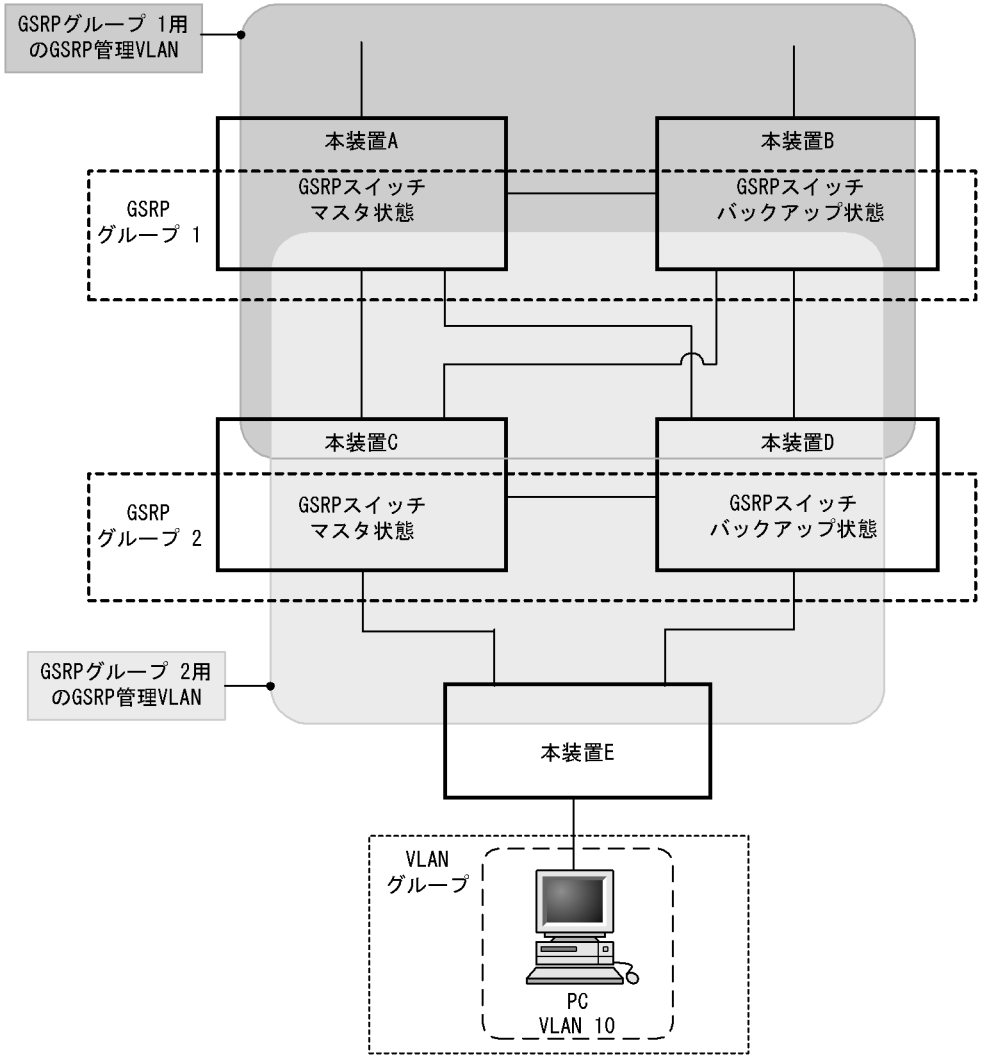


14.4.2　GSRP グループの多段構成

GSRP では，同一のレイヤ 2 ネットワーク内に複数の GSRP グループを多段にした構成をとることができ

ます。これによって大規模ネットワークでも，冗長性を確保できます。GSRP グループを多段構成にする場合，GSRP の制御フレームの送信範囲を限定するため，GSRP グループごとに GSRP 管理 VLAN を設定します。GSRP グループの多段構成の概要を次の図に示します。

図 14-9　GSRP グループの多段構成



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

14.5 GSRP 使用時の注意事項

(1) 他機能との共存について

GSRP との共存で制限のある機能を次の表に示します。

表 14-4 GSRP との共存で制限のある機能

制限のある機能	制限の内容
シングルスパニングツリー	共存不可
PVST+	
マルチプルスパニングツリー	
IEEE802.1X	
アップリンク・リダンダント	

(2) ポートリセット機能を使用する場合について

ポートリセット機能を設定したポートと対向のスイッチとの間に伝送装置などを設置した場合，対向のスイッチで正しくポートのリンクダウンを検出できないおそれがあります。

ポートリセット機能を使用する場合は，対向のスイッチでポートのリンクダウンが直接検出できるようにネットワークの設計を行ってください。

(3) ポートリセット機能をロードバランス構成で使用する場合について

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

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

(4) GSRP 使用時の VLAN 構成について

GSRP 使用時は，すべての VLAN が GSRP によって制御されます。そのため，VLAN グループに属していない VLAN のポートは，ブロッキング状態になります。VLAN グループに属している VLAN だけを制御する場合は，GSRP VLAN グループ限定制御機能を使用してください。

(5) GSRP VLAN グループ限定制御機能について

次に示す動作が行われた場合，GSRP VLAN グループ限定制御機能を設定していても，すべての VLAN が一時的にダウンします。このとき VLAN のポートはブロッキング状態になります。

- コンフィグレーションコマンド gsrp で，GSRP グループ ID を設定
- 運用コマンド restart gsrp の実行

(6) ダイレクトリンク障害検出機能について

ダイレクトリンクで本装置との間に伝送装置などを設置した構成で伝送装置の障害が発生した場合，マス

タ状態で稼働中の本装置は正常に動作しているにもかかわらず，バックアップ状態で稼働中の別の本装置は対向の本装置で障害が発生したと認識し，自動でマスタ状態へ切り替わる可能性があります。この結果，2 台の本装置で同時にマスタ状態となります。また，ダイレクトリンクの片線切れ障害が発生した場合でも同様の現象が発生するおそれがあります。そのため，コンフィグレーションコマンド no-neighbor-to-master で direct-down を指定する場合は，ダイレクトリンクを冗長構成にし，複数経路で GSRP advertise フレームの送受信ができるようネットワークの設計をしてください。なお，ダイレクトリンクを冗長構成にするためには，リンクアグリゲーションを使用する方法，通常のポートを複数使用する方法などがありますが，どちらも効果は同じです。

(7) GSRP 使用時のネットワークの構築について

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

- GSRP のコンフィグレーションを設定する際，事前に本装置のポートを shutdown に設定するなどダウン状態にしてください。コンフィグレーション設定後，GSRP の状態遷移が安定したあとで，運用を開始してください。
- GSRP グループを構成する 2 台の本装置のうち 1 台だけを起動させて，コンフィグレーションを設定し，バックアップ状態に切り替わったことを確認したあとで，もう一方の GSRP スイッチを起動してコンフィグレーションを設定してください。
- GSRP VLAN グループ限定制御機能を設定している場合，VLAN グループに属していない VLAN はアップ状態です。VLAN グループに VLAN を所属させる場合は，その VLAN の状態をあらかじめ disable にして，VLAN グループの状態が定まったあとに VLAN の状態を enable にしてください。VLAN グループから VLAN を削除する場合も，その VLAN の状態をあらかじめ disable にして，ループが発生しないように運用してください。

(8) GSRP 使用中の VLAN 構成の変更について

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

このような切り替えを防止するためには，VLAN の構成を変更する際には次に示すような対応をしてください。

- マスタ，バックアップの選択基準の優先順（コンフィグレーションコマンド selection-pattern）を，優先度を最高優先順とするように設定し，優先度の設定でマスタを固定にした状態でコンフィグレーションを設定してください。
- ケーブル配線の変更や装置の再起動を伴うような大きな構成変更が必要な場合などには，バックアップ固定機能を使って片方の GSRP スイッチを強制的にバックアップ状態にし，もう一方の GSRP スイッチをすべての VLAN グループのマスタとした状態で構成変更を行ってください。

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

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

(10) GSRP Flush request フレームの中継について

GSRP aware は GSRP Flush request フレームをフラッディングします。GSRP aware で GSRP Flush request フレームを中継させるネットワーク構成では，GSRP aware のソフトウェアバージョンを Ver.10.4 以降にする必要があります。GSRP スイッチは GSRP Flush request フレームをフラッディングしないので，GSRP グループの多段構成などで GSRP スイッチでの GSRP Flush request フレームを中継させる構成はできません。

(11) GSRP 使用時の本装置のリモート管理について

GSRP を使用する本装置に対して，telnet や SNMP などのリモート管理をする場合，次に示す方法を使用してください。

- GSRP 制御対象外ポート
- GSRP VLAN グループ限定制御機能を設定し，VLAN グループに属さない VLAN の VLAN インタフェース

(12) GSRP 制御対象外ポートについて

GSRP 制御対象外ポートに設定したポートは，マスタ／バックアップ状態に関係なく，常時通信可能なポートとなります。このため，GSRP 制御対象外ポートに設定したポートに属する VLAN の IP インタフェースもアップ状態となります。

(13) 相互運用

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

(14) CPU 過負荷時

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

(15) VLAN グループ設定上の注意

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

15 GSRP の設定と運用

この章では，GSRP 機能の設定例について説明します。

15.1 コンフィグレーション

15.1.1 コンフィグレーションコマンド一覧

GSRP 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 15-1 コンフィグレーションコマンド一覧

コマンド名	説明
advertise-holdtime	GSRP Advertise フレームの保持時間を設定します。
advertise-interval	GSRP Advertise フレームの送信間隔を設定します。
backup-lock	バックアップ固定機能を設定します。
flush-request-count	GSRP Flush request フレームの送信回数を設定します。
gsrp	GSRP を設定します。
gsrp-vlan	GSRP 管理 VLAN を設定します。
gsrp direct-link	ダイレクトリンクを設定します。
gsrp exception-port	GSRP 制御対象外ポートを設定します。
gsrp limit-control	GSRP VLAN グループ限定制御機能を設定します。
gsrp no-flush-port	GSRP Flush request フレームを送信しないポートを設定します。
gsrp reset-flush-port	ポートリセット機能を使用するポートを設定します。
no-neighbor-to-master	バックアップ（隣接不明）状態となったときの切り替え方法を設定します。
port-up-delay	リンク不安定時の連続切り替え防止機能を設定します。
reset-flush-time	ポートリセット機能使用時のリンクダウン時間を設定します。
selection-pattern	マスタ，バックアップの選択基準の優先順を設定します。
vlan-group disable	VLAN グループを無効にします。所属している VLAN は通信が停止します。
vlan-group priority	VLAN ごとの優先度を設定します。
vlan-group vlan	VLAN グループに所属する VLAN を設定します。

15.1.2 GSRP の基本的な設定

(1) GSRP グループの設定

[設定のポイント]

GSRP を使用するために，本装置の GSRP グループ ID を設定します。GSRP グループ ID を設定すると本装置で GSRP の動作を開始します。番号は隣接する GSRP スイッチと合わせて設定します。GSRP を設定するためには，事前にスパニングツリーを停止する必要があります。

[コマンドによる設定]

1. **(config)# spanning-tree disable**
   スパニングツリーを停止します。

2. **(config)# gsrp 1**
   GSRP グループ ID を 1 に設定します。本コマンドによって，本装置は GSRP の動作を開始します。

[注意事項]

GSRP VLAN グループ限定制御機能を設定していない場合，GSRP グループ ID を設定すると，すべての VLAN を GSRP で制御します。VLAN グループを設定していない状況では，すべての VLAN のポートがブロッキング状態になります。

(2) GSRP 管理 VLAN の設定

[設定のポイント]

GSRP 管理 VLAN として使用する VLAN を指定します。設定しない場合，GSRP 管理 VLAN は 1 となります。

GSRP 管理 VLAN は GSRP の制御フレームをやり取りするための VLAN です。この VLAN には，GSRP スイッチ間のダイレクトリンクと，GSRP aware を使用する場合はそのスイッチとの接続ポートを設定してください。また，GSRP aware にも GSRP スイッチと接続しているポートで同じ VLAN を設定してください。

[コマンドによる設定]

1. **(config)# gsrp 1**

   GSRP コンフィグレーションモードに移行します。

2. **(config-gsrp)# gsrp-vlan 5**

   GSRP 管理 VLAN として VLAN 5 を使用します。

(3) ダイレクトリンクの設定

[設定のポイント]

GSRP のダイレクトリンクに使用するポートを設定します。ダイレクトリンクは，イーサネットインタフェースまたはポートチャネルインタフェースに設定します。

ダイレクトリンク障害検出機能を使用する場合，対向装置の装置障害以外でダイレクトリンク障害となる可能性を少なくするため，ダイレクトリンクを冗長構成にすることをお勧めします。ダイレクトリンクを冗長構成にするためには，リンクアグリゲーションを使用する方法と通常のリンクを複数使用する方法があり，どちらも効果は同じです。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 0/1-2**

   ポート 0/1，0/2 のイーサネットインタフェースコンフィグレーションモードに移行します。ダイレクトリンクを冗長化するために複数のポートを指定します。

2. **(config-if-range)# channel-group 10 mode on**
   (config-if-range)# exit

   ポート 0/1，0/2 をスタティックモードのチャネルグループ 10 に登録します。

3. **(config)# interface port-channel 10**
   (config-if)# gsrp 1 direct-link

   GSRP グループ ID1 のダイレクトリンクとしてチャネルグループ 10 を設定します。

(4) VLAN グループの設定

[設定のポイント]

GSRP で運用する VLAN グループと VLAN グループに所属する VLAN を設定します。マスタ状態の VLAN グループに所属した VLAN で通信可能となります。VLAN グループは複数設定でき，VLAN グループごとにマスタ，バックアップを制御します。VLAN グループと所属する VLAN は，隣接する GSRP スイッチと同じ設定をしてください。
VLAN グループへの VLAN の追加および削除は，vlan-group vlan add コマンドおよび vlan-group vlan remove コマンドで行います。vlan-group vlan コマンドを設定済みの状態でもう一度 vlan-group vlan コマンドを実行すると，指定した VLAN ID リストに置き換わります。
VLAN グループの通信を停止したい場合，vlan-group disable コマンドで VLAN グループを無効にできます。

[コマンドによる設定]

1. **(config)# gsrp 1**
   GSRP コンフィグレーションモードに移行します。

2. **(config-gsrp)# vlan-group 1 vlan 10,20**
   VLAN グループ 1 を設定し，VLAN 10，20 を VLAN グループ 1 に所属させます。

3. **(config-gsrp)# vlan-group 1 vlan add 30**
   VLAN グループ 1 に所属する VLAN に VLAN 30 を追加します。

4. **(config-gsrp)# vlan-group 1 vlan remove 20**
   VLAN グループ 1 に所属する VLAN から VLAN 20 を削除します。

5. **(config-gsrp)# vlan-group 1 vlan 100,200**
   VLAN グループ 1 に所属する VLAN を VLAN 100，200 に設定します。以前の設定はすべて上書きされて，VLAN 100，200 が所属する VLAN となります。

[注意事項]

VLAN グループに属していない VLAN の動作は，GSRP VLAN グループ限定制御機能の設定によって異なります。
GSRP VLAN グループ限定制御機能を設定していない場合は，GSRP ではすべての VLAN が GSRP によって制御されます。そのため，VLAN グループに属していない VLAN のポートは，ブロッキング状態になります。
GSRP VLAN グループ限定制御機能を設定している場合は，VLAN グループに所属している VLAN だけを GSRP の制御対象にします。そのため，VLAN グループに属していない VLAN のポートは，フォワーディング状態になります。

15.1.3 マスタ，バックアップの選択に関する設定

(1) マスタ，バックアップの選択方法の設定

[設定のポイント]

GSRP のマスタ，バックアップ状態を切り替えるときの，選択基準（アクティブポート数，優先度，装置 MAC アドレス）の優先順を設定します。優先順は，アクティブポート数→優先度→装置 MAC アドレスの順番と優先度→アクティブポート数→装置 MAC アドレスの順番のどちらかを選択します。
通常，アクティブポート数を最優先とすることをお勧めします。ネットワーク構成を変更する際に VLAN のポート数の増減やリンクダウンなどを伴う作業を行う場合，優先度を最優先とする設定に

よってマスタ，バックアップの状態を固定したまま作業を行えます。

[コマンドによる設定]

1. **(config)# gsrp 1**
   GSRP コンフィグレーションモードに移行します。

2. **(config-gsrp)# selection-pattern priority-ports-mac**
   選択基準の優先順位を，優先度→アクティブポート数→装置 MAC アドレスの順に設定します。

(2) VLAN グループの優先度の設定

[設定のポイント]

VLAN グループごとに，優先度を設定します。数字が大きいほど優先度が高くなります。優先度を設定することによって，アクティブポート数が同じ状態でマスタにしたい装置を設定します。
複数の VLAN グループを作成し，VLAN グループごとに優先度を変えることで，VLAN グループごとのロードバランス構成をとることができます。

[コマンドによる設定]

1. **(config)# gsrp 1**
   GSRP コンフィグレーションモードに移行します。

2. **(config-gsrp)# vlan-group 1 priority 80**
   VLAN グループ 1 の優先度を 80 に設定します。

(3) バックアップ固定機能の設定

[設定のポイント]

バックアップ固定機能は，片方の GSRP スイッチの全 VLAN グループを強制的にバックアップ状態にします。ケーブル配線の変更や装置の再起動を伴うような大きな構成変更を行いたい場合などに，本機能によって対向の GSRP スイッチをすべての VLAN グループのマスタとした状態で構成変更を行えます。

[コマンドによる設定]

1. **(config)# gsrp 1**
   GSRP コンフィグレーションモードに移行します。

2. **(config-gsrp)# backup-lock**
   バックアップ固定機能を設定します。すべての VLAN グループがバックアップになり，対向の GSRP スイッチがマスタになります。

15.1.4 GSRP VLAN グループ限定制御機能の設定

[設定のポイント]

GSRP VLAN グループ限定制御機能を設定します。GSRP VLAN グループ限定制御機能は，VLAN グループに所属している VLAN だけを GSRP の制御対象にします。VLAN グループに所属していない VLAN のポートは，常にフォワーディング状態になります。

GSRP VLAN グループ限定制御機能は，次の用途で使用できます。
- GSRP の VLAN グループに所属していない VLAN を GSRP 制御の対象外として運用
- 本装置のリモート管理

[コマンドによる設定]

1. **(config)# gsrp limit-control**
   GSRP VLAN グループ限定制御機能を設定します。

15.1.5 GSRP 制御対象外ポートの設定

[設定のポイント]

ポートまたはリンクアグリゲーションに対して GSRP 制御対象外ポートを設定します。イーサネットインタフェースまたはポートチャネルインタフェースに対して設定し，設定すると GSRP の状態に関係なく常にフォワーディング状態になります。
GSRP 制御対象外ポートは，次の用途で使用できます。
- 本装置のリモート管理用ポート

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# gsrp exception-port**
   ポート 0/1 を GSRP 制御対象外ポートとして設定します。

15.1.6 GSRP のパラメータの設定

(1) リンク不安定時の連続切り替え防止機能の設定

GSRP ではマスタ，バックアップの選択要因として，アクティブポート数を使用します。そのため，ポートのアップ，ダウンが頻発するなどのポートが不安定な状態となった場合にアクティブポート数の増減が多発し，その結果，マスタ状態とバックアップ状態の切り替えが連続して発生するおそれがあります。
ポートが不安定な状態の際，本コマンドで遅延時間を指定することで，不要な切り替えを抑止できます。

[設定のポイント]

ポートがアップした場合にアクティブポート数のカウント対象に反映するまでの遅延時間を設定します。
パラメータに infinity を指定した場合は，遅延時間を無限とし，自動ではアクティブポートにカウントしません。設定しない場合，ポートがアップするとアクティブポート数のカウント対象に即時反映（0 秒）します。

[コマンドによる設定]

1. **(config)# gsrp 1**
   GSRP コンフィグレーションモードに移行します。

2. **(config-gsrp)# port-up-delay 10**
   アクティブポート数へのカウント対象に反映する遅延時間を 10 秒に設定します。

3. **(config-gsrp)# port-up-delay infinity**
   アクティブポート数へのカウント対象に反映する遅延時間を無限に変更します。この設定の場合，ポートのアップ後にカウント対象に反映するためには clear gsrp port-up-delay コマンドを使用してください。

(2) GSRP Advertise フレームの送信間隔，保持時間の設定

[設定のポイント]

GSRP Advertise フレームの送信間隔および保持時間を設定します。advertise-holdtime は advertise-interval より大きな値を設定してください。advertise-interval 以下の値を設定した場合，GSRP Advertise フレームの受信タイムアウトを検出します。

[コマンドによる設定]

1. **(config)# gsrp 1**
   GSRP コンフィグレーションモードに移行します。

2. **(config-gsrp)# advertise-interval 5**
   GSRP Advertise フレームの送信間隔を 5 秒に設定します。

3. **(config-gsrp)# advertise-holdtime 20**
   GSRP Advertise フレームの保持時間を 20 秒に設定します。この場合，GSRP Advertise フレームの未到達を 3 回まで許容します。

[注意事項]

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

(3) GSRP Flush request フレームを送信しないポートの設定

[設定のポイント]

ポートまたはリンクアグリゲーションに対して GSRP Flush request フレームを送信しないポートを設定します。イーサネットインタフェースまたはポートチャネルインタフェースに対して設定します。GSRP Flush request は GSRP 管理 VLAN のうちダイレクトリンクおよびポートリセット機能を設定しているポート以外の全ポートに送信します。本機能は GSRP unaware との接続でポートリセット機能を使用したくない場合に設定します。ただし，このような構成ではマスタ，バックアップの切り替え時に GSRP unaware の MAC アドレステーブルがエージングによってクリアされるまで通信が復旧しないことに注意してください。通常は，GSRP unaware との接続にはポートリセット機能を使用することをお勧めします。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# gsrp 1 no-flush-port**
   ポート 0/1 から GSRP Flush request フレームを送信しないように設定します。

(4) GSRP Flush request フレームの送信回数の設定

[設定のポイント]

周囲のスイッチに対して MAC アドレステーブルのクリアを行う GSRP Flush request フレームの送信回数を指定します。
デフォルトは 3 回 GSRP Flush request を送信します。回数を増やすと，フレームのロスに対して耐性を高めることができます。

[コマンドによる設定]

1. **(config)# gsrp 1**
   GSRP コンフィグレーションモードに移行します。

2. **(config-gsrp)# flush-request-count 5**
   GSRP Flush request フレームの送信回数を 5 回に設定します。

15.1.7 ポートリセット機能の設定

本機能は GSRP unaware との接続に使用します。マスタ，バックアップの切り替えでバックアップ状態になった装置はポートリセット機能を設定したポートを一時的にリンクダウンします。

(1) 適用するポートの設定

[設定のポイント]

ポートリセット機能を設定します。イーサネットインタフェースまたはポートチャネルインタフェースに対して設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# gsrp 1 reset-flush-port**
   ポート 0/1 にポートリセット機能を設定します。

(2) ポートダウン時間の設定

[設定のポイント]

ポートリセット機能使用時のポートダウン時間を設定します。デフォルトは 3 秒です。ポートリセット機能を使用する場合に，対向装置のリンクダウン検出時間が長いときに設定します。本装置のリンクダウン検出タイマ機能（コンフィグレーションコマンド link debounce）のようにリンクダウン検出時間を設定できる装置と接続している場合，その時間より長く設定してください。

[コマンドによる設定]

1. **(config)# gsrp 1**
   GSRP コンフィグレーションモードに移行します。

2. **(config-gsrp)# reset-flush-time 5**

ポートダウン時間を 5 秒に設定します。

15.1.8 ダイレクトリンク障害検出の設定

[設定のポイント]

ダイレクトリンクの障害によってバックアップ（隣接不明）状態からマスタ状態に切り替えるときに，手動（マスタ遷移コマンド入力）で切り替えるか，自動（ダイレクトリンク障害検出機能）で切り替えるかを選択します。

ダイレクトリンク障害検出機能を使用し自動で切り替える場合，対向装置の装置障害以外でダイレクトリンク障害と検出する可能性を少なくするため，ダイレクトリンクを冗長構成にすることをお勧めします。ダイレクトリンクを冗長構成にするためには，リンクアグリゲーションを使用する方法と通常のリンクを複数使用する方法があり，どちらも効果は同じです。

[コマンドによる設定]

1. **(config)# gsrp 1**
   GSRP コンフィグレーションモードに移行します。

2. **(config-gsrp)# no-neighbor-to-master direct-down**
   ダイレクトリンク障害検出機能を設定し，ダイレクトリンクの障害時に自動でマスタ状態に遷移します。

15.2 オペレーション

15.2.1 運用コマンド一覧

GSRP の運用コマンド一覧を次の表に示します。

表 15-2 運用コマンド一覧

コマンド名	説明
show gsrp	GSRP 情報を表示します。
show gsrp aware	GSRP の aware 情報を表示します。
clear gsrp	GSRP の統計情報をクリアします。
set gsrp master	バックアップ（隣接不明）状態をマスタ状態に遷移させます。
clear gsrp port-up-delay	VLAN グループに定義されている VLAN に属しているポートでアップ状態となったポートを，コンフィグレーションコマンド port-up-delay で指定された遅延時間を待たないで，即時アクティブポートへ反映します。
clear gsrp forced-shift	GSRP スイッチ単独起動時のマスタ遷移機能による，自動マスタ遷移待ち状態を解除します。
restart gsrp	GSRP プログラムを再起動します。
dump protocols gsrp	GSRP プログラムで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

15.2.2 GSRP の状態の確認

本装置で GSRP の機能を使用した場合の確認内容には次のものがあります。

(1) コンフィグレーション設定後の確認

show gsrp コマンドで GSRP の設定の状態を確認できます。コンフィグレーションで設定した GSRP の設定内容が正しく反映されているかどうかを確認してください。また，本装置と同一 GSRP グループを構成する相手装置との間でマスタ，バックアップ選択方法（Selection Pattern），VLAN グループ ID（VLAN Group ID），および VLAN グループに所属する VLAN が同一であることを確認してください。

show gsrp detail コマンド，show gsrp vlan-group コマンドの表示例を次に示します。

図 15-1 show gsrp detail コマンドの実行結果

```
> show gsrp detail
Date 2008/11/07 22:24:36 UTC

GSRP ID: 1
 Local MAC Address        : 0012.e205.0000
 Neighbor MAC Address     : 0012.e205.0011
 Total VLAN Group Counts : 2
 GSRP VLAN ID             : 105
 Direct Port              : 0/10-11
 Limit Control            : Off
 GSRP Exception Port      : 0/1-5
 No Neighbor To Master    : manual
 Backup Lock              : disable
 Port Up Delay            : 0
 Last Flush Receive Time : -
 Forced Shift Time        : -

                            Local               Neighbor
 Advertise Hold Time      : 5                   5
 Advertise Hold Timer     : 4                   -
 Advertise Interval       : 1                   1
 Selection Pattern        : ports-priority-mac  ports-priority-mac

 VLAN Group ID      Local State         Neighbor State
 1                  Backup              Master
 8                  Master              Backup
>
```

図 15-2 show gsrp vlan-group コマンドの実行結果

```
> show gsrp 1 vlan-group 1
Date 2005/11/07 22:25:13 UTC

GSRP ID: 1
 Local MAC Address        : 0012.e205.0000
 Neighbor MAC Address     : 0012.e205.0011
 Total VLAN Group Counts : 1

 VLAN Group ID : 1
  VLAN ID                 : 110,200-210
  Member Port             : 0/6-8
  Last Transition         : 2005/11/07 22:20:11  (Master to Backup)
  Transition by reason    : Priority was lower than neighbor's
  Master to Backup Counts : 4
  Backup to Master Counts : 4


                            Local               Neighbor
  State                   : Backup              Master
  Acknowledged State      : Backup              -
  Advertise Hold Timer    : 3                   -
  Priority                : 100                 101
  Active Ports            : 3                   3
  Up Ports                : 3                   -
>
```

(2) 運用中の確認

本装置および本装置と同一 GSRP グループを構成する相手装置で，VLAN グループの状態がどれかの装置で Master になっていること，および同一 VLAN グループで複数のマスタが存在しないことを確認してください。本装置での VLAN グループの状態確認には show gsrp コマンドを使用してください。

図 15-3 show gsrp コマンドの実行例

```
> show gsrp
Date 2005/11/07 22:28:38 UTC

GSRP ID: 10
 Local MAC Address       : 0012.e205.0000
 Neighbor MAC Address    : 0012.e205.0011
 Total VLAN Group Counts : 2

 VLAN Group ID      Local State         Neighbor State
 1                  Backup              Master
 8                  Master              Backup
>
```

15.2.3 コマンドによる状態遷移

set gsrp master コマンドで，バックアップ（隣接不明）状態をマスタ状態に遷移させることができます。

このコマンドは，バックアップ（隣接不明）状態のときだけ有効なコマンドです。対向装置の該当する VLAN グループ状態がバックアップになっていることを確認したあとに実行してください。

図 15-4 set gsrp master コマンドの実行結果

```
> set gsrp master 1 vlan-group 1
Transit to Master. Are you sure? (y/n):y
>
```

15.2.4 遅延状態のポートのアクティブポート即時反映

clear gsrp port-up-delay コマンドで，リンク不安定時の連続切り替え防止機能（コンフィグレーションコマンド port-up-delay）を使用している場合に，ポートアップ後の遅延時間を待たないですぐにアクティブポートへ反映できます。

図 15-5 clear gsrp port-up-delay コマンドの実行結果

```
> clear gsrp port-up-delay port 0/1
>
```

16 アップリンク・リダンダント

アップリンク・リダンダントは，アップリンクに使用する二つのポートのうち，どちらか一方で通信し，もう一方を障害時用に待機させることで，冗長化構成ができるようにするための機能です。アップリンクのポートには，物理ポートまたはリンクアグリゲーションを設定できます。
この章では，アップリンク・リダンダントの解説と操作方法について説明します。

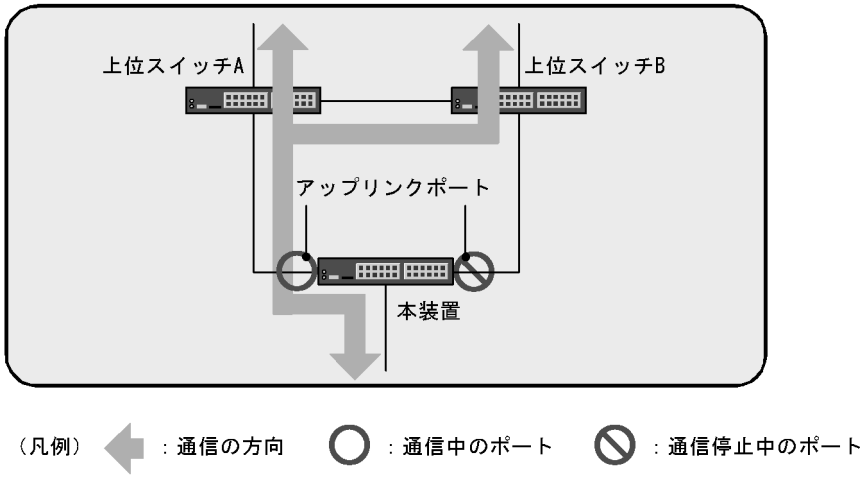
16.1 解説

16.1.1 概要

アップリンク・リダンダントは，本装置でアップリンクに用いるポートを二重化し，通信中にリンク障害が起こったときは待機中のポートに切り替えて上位スイッチとの通信を継続する機能です。本機能を使用すると，スパニングツリーなどの複雑なプロトコルを使わないでアップリンクに用いるポートを冗長化できます。冗長化するための二つのポートをあわせて，**アップリンクポート**と呼びます。

アップリンク・リダンダントの基本構成を次の図に示します。

図 16-1 アップリンク・リダンダントの基本構成



この図の構成でアップリンク・リダンダントを使用した場合，本装置と上位スイッチ A との間のリンクに障害が発生しても，本装置と上位スイッチ B との間のリンクに切り替えることで通信を継続できます。

16.1.2 サポート仕様

アップリンク・リダンダントでのサポート状況を次の表に示します。

表 16-1 アップリンク・リダンダントでのサポート状況

項目		サポート有無・仕様
適用インタフェース	物理ポート	○
	リンクアグリゲーション	○
アップリンクポート数		25
一つのアップリンクポートに設定可能なインタフェース数		2
プライマリポートへのアクティブポート自動切り戻し		○
プライマリポートへのアクティブポート自動切り戻し抑止		○
アクティブポート変更コマンド		○
アクティブポート変更時のフラッシュ制御フレーム送受信		○
アクティブポート変更時の MAC アドレスアップデート		○
起動時のアクティブポート固定		○
プライベート MIB，プライベートトラップ		○

（凡例）○：サポート

16.1.3 アップリンク・リダンダント動作概要

アップリンク・リダンダントでは，1 対のポートまたはリンクアグリゲーションを用いて冗長性を確保します。このポート対がアップリンクポートです。アップリンクポートには，通常，通信を行うプライマリポートと，プライマリポートの障害時に通信を行うセカンダリポートの二つがあります。これらのポートは，コンフィグレーションで設定します。

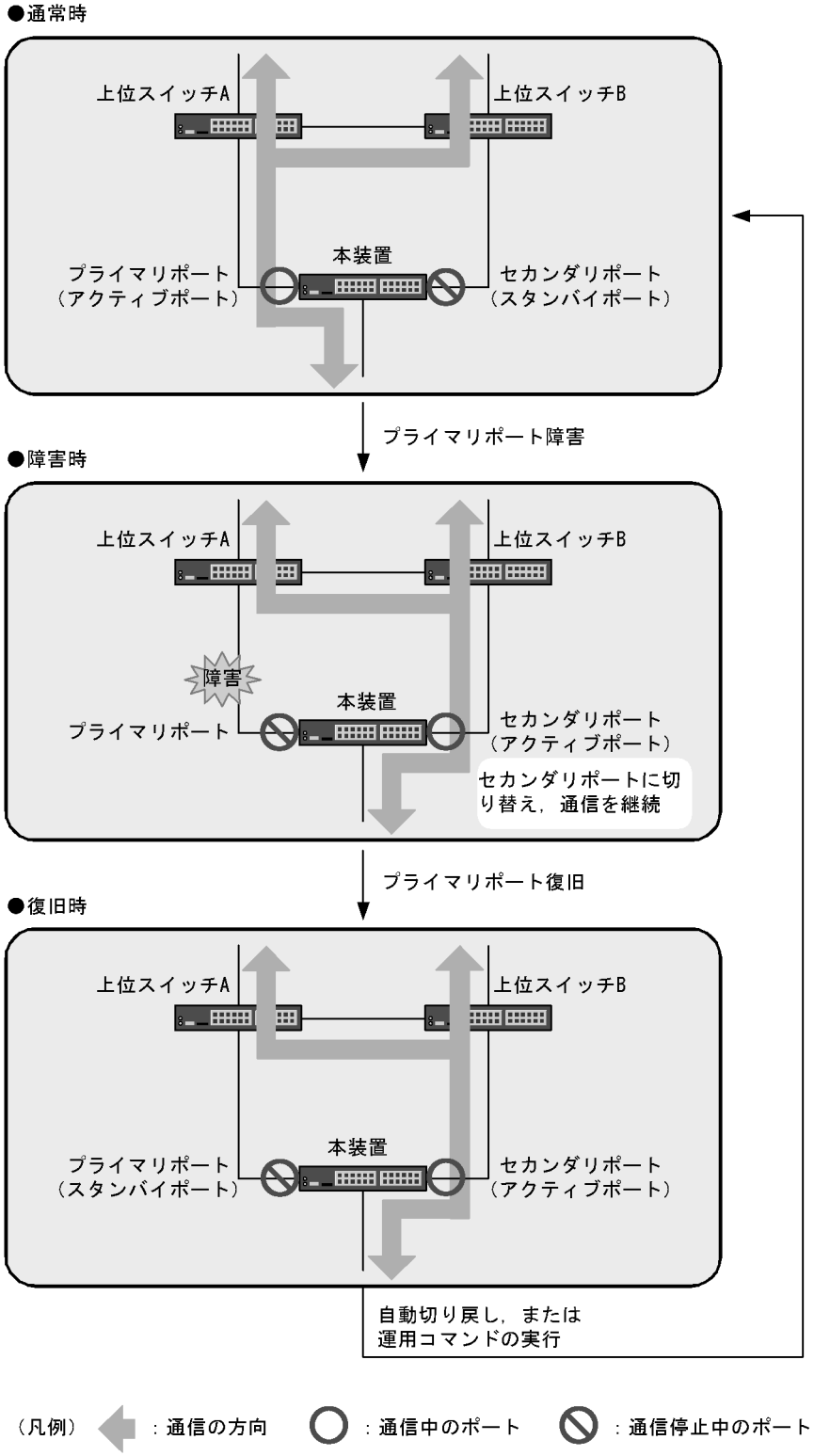
プライマリポートとセカンダリポートは，同じ帯域やポート数である必要はありません。例えば，プライマリポートには 10 ギガビット・イーサネットポートを，セカンダリポートには 1 ギガビット・イーサネットポートを 5 本束ねたリンクアグリゲーションを設定することもできます。

アップリンクポートのうち，現在通信を行っているポートをアクティブポートと呼びます。また，アクティブポートに障害が発生した場合に，通信継続のため，すぐに通信を開始できるような準備ができているポートをスタンバイポートと呼びます。

アップリンクポートを構成する 1 対のポートは，VLAN などの構成を同一設定にする必要があります。また，アップリンクポートに設定しているポートは，ほかのアップリンクポートでは設定できません。

アップリンク・リダンダントの動作概要を次の図に示します。

図 16-2 アップリンク・リダンダントの動作概要



通常時

本装置のプライマリポートを経由して，上位スイッチへ通信できる状態です。本装置のセカンダリポートは通信していない状態です。

障害時

プライマリポートのリンクダウンを契機に，本装置がアクティブポートをセカンダリポートに変更し，セカンダリポートを経由して上位スイッチへの通信を継続します。この動作を切り替えと呼びます。このとき，新しくアクティブポートになったセカンダリポートから上位スイッチへ，フラッシュ制御フレームという専用の制御フレームまたはMACアドレスアップデートフレームを送信することで，上位スイッチのMACアドレステーブルを更新し，通信を速やかに復旧できます。

復旧時

プライマリポートがリンクアップしてスタンバイポートになっていれば，自動切り戻し機能を使用する，または本装置で運用コマンドを実行することで，アクティブポートをプライマリポートに変更できます。この動作を切り戻しと呼びます。
また，切り替え時と同様に，フラッシュ制御フレームまたはMACアドレスアップデートフレームを送信することで，通信を速やかに復旧できます。

16.1.4 切り替え・切り戻し動作

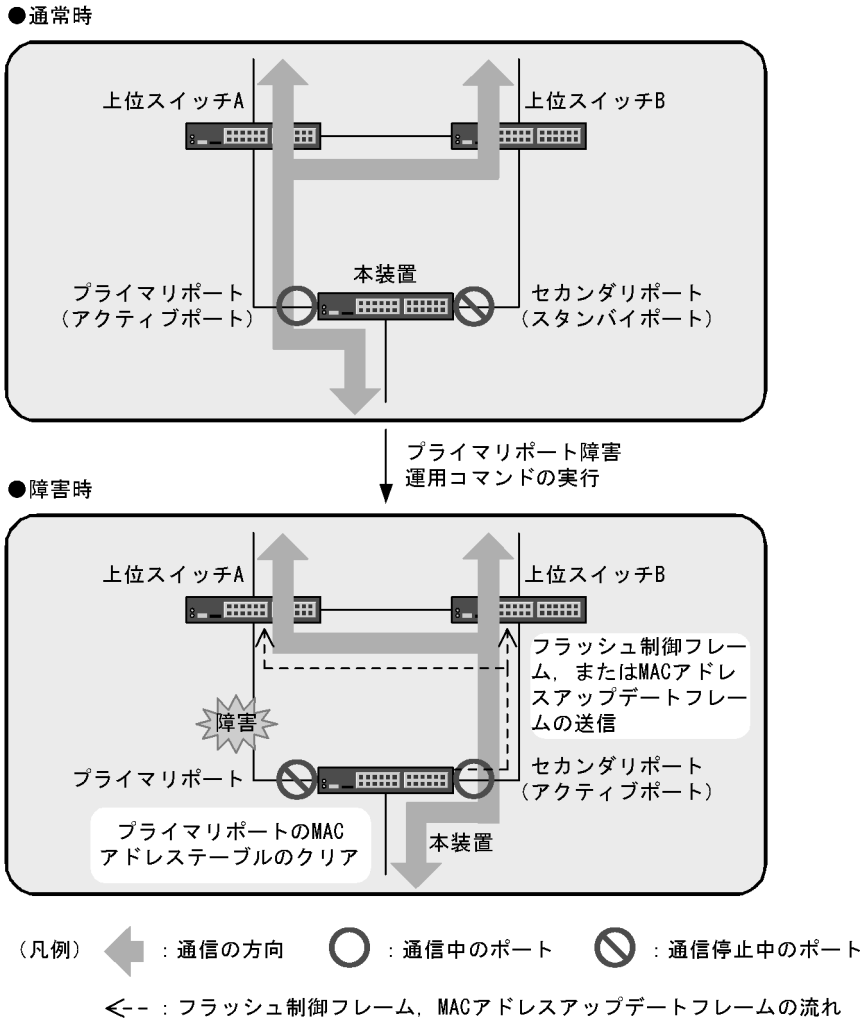
切り替え・切り戻しとは，通信を行っているポートを変更する動作です。切り替え・切り戻しは，アクティブポートの変更先ポートがスタンバイポートとなっている場合に，次の契機で動作します。

- アクティブポートに障害が発生する
- 自動切り戻し機能の待ち時間が経過する
- アクティブポートを変更する運用コマンドを実行する

切り替え・切り戻し動作と同時に，通信を行っていたポートで学習していたMACアドレスをすべてクリアして，新しくアクティブポートになったポートで通信を行います。フラッシュ制御フレームまたはMACアドレスアップデートフレームを送信する設定をしている場合は，切り替え・切り戻しと同時に新しくアクティブポートになったポートからフラッシュ制御フレームまたはMACアドレスアップデートフレームを送信します。

切り替え動作を次の図に示します。

図 16-3 切り替え動作



16.1.5 自動切り戻し機能

自動切り戻し機能とは，プライマリポートの障害によってセカンダリポートがアクティブポートになっている状態で，プライマリポートが障害から復旧した場合に，自動的にアクティブポートをプライマリポートに変更する機能です。切り戻しの待ち時間は，0 秒（即時）から 300 秒の間で設定できます。

運用コマンドによってアクティブポートを変更した場合，自動切り戻しは動作しません。ただし，次のどちらかの条件を満たす場合には自動切り戻しが動作します。

- 運用コマンドによってアクティブポートを変更したあとで，コンフィグレーションで本機能を設定または変更した場合
- 運用コマンドによってアクティブポートを変更したあとで，プライマリポートの障害が発生または回復した場合

16.1.6 通信復旧の補助機能

アップリンク・リダンダントでは，切り替え・切り戻し動作時に通信復旧を補助する二つの機能をサポートしています。なお，一つのアップリンクポートに設定できる機能はどちらか一つだけです。

● フラッシュ制御フレーム送受信機能

フラッシュ制御フレームを送信することで，上位スイッチの MAC アドレステーブルをクリアして，フラッディングによって通信を復旧します。上位スイッチは，フラッシュ制御フレームによる MAC アドレステーブルのクリアをサポートしている必要があります。

- MAC アドレスアップデート機能
  MAC アドレスアップデートフレームを送信することで，上位スイッチに端末の MAC アドレスを再学習させて通信を復旧します。上位スイッチに専用の受信機能は必要ありませんが，再学習させられる MAC アドレス数に制限があります。また，通信を復旧するまでに 10 秒程度時間が掛かる場合があります。

フラッシュ制御フレーム送受信機能は，上位スイッチがフラッシュ制御フレームをサポートしている装置を想定しているのに対して，MAC アドレスアップデート機能は，フラッシュ制御フレームを受信できない装置を想定しています。

16.1.7 フラッシュ制御フレーム送受信機能

(1) 送信動作

通信を行っているリンクの障害や運用コマンドによって，アクティブポートを変更した場合，通信を速やかに復旧させるために，上位スイッチの MAC アドレステーブルをクリアするフラッシュ制御フレームを送信できます。フラッシュ制御フレームの送信は，アップリンクポートごとに設定でき，送信先の VLAN を指定できます。

MAC アドレステーブルをクリアしたくない装置がネットワーク上にある場合には，フラッシュ制御フレームを送受信する専用の VLAN を作成し，その VLAN にフラッシュ制御フレームを送信するように設定することで，MAC アドレステーブルをクリアする装置の範囲を制限できます。

本装置はフラッシュ制御フレームを，アクティブポートの変更直後に，新しくアクティブポートになったポートから送信します。

トランクポートでフラッシュ制御フレームを送信する場合には，送信先の VLAN を指定する必要があります。アクセスポート，MAC ポートまたはプロトコルポートの場合には，送信先 VLAN の指定の有無に関係なく，Untagged フレームのフラッシュ制御フレームを送信します。

(2) 受信動作

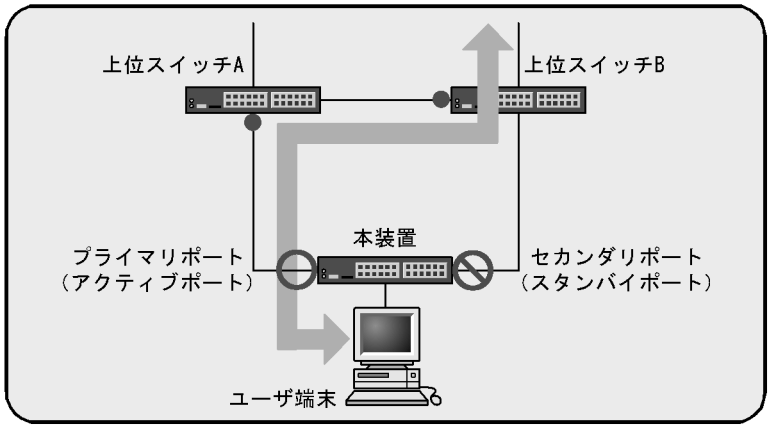
本装置は，フラッシュ制御フレームを受信すると MAC アドレステーブルをクリアします。

フラッシュ制御フレームを受信するためのコンフィグレーションは必要ありません。ただし，特定の VLAN にフラッシュ制御フレームを送信する設定となっている場合には，その VLAN でフラッシュ制御フレームが通信できる状態となっている必要があります。

フラッシュ制御フレームの使用による切り替え動作の違いを次の図に示します。

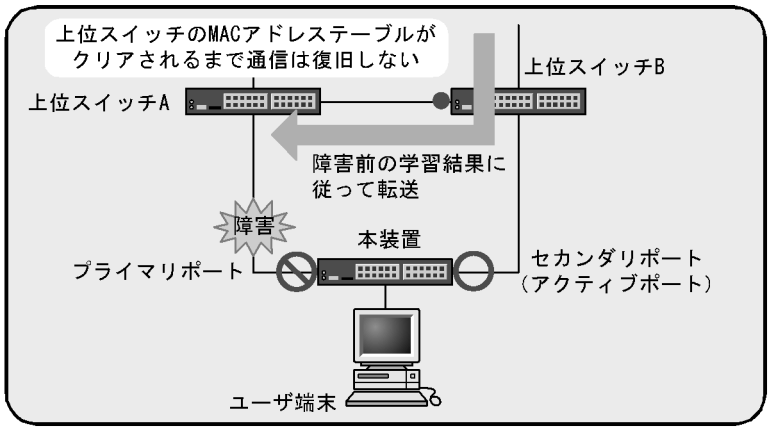
図 16-4 フラッシュ制御フレームの使用による切り替え動作の違い

●通常時（上位スイッチA，Bを経由するデータの流れ）

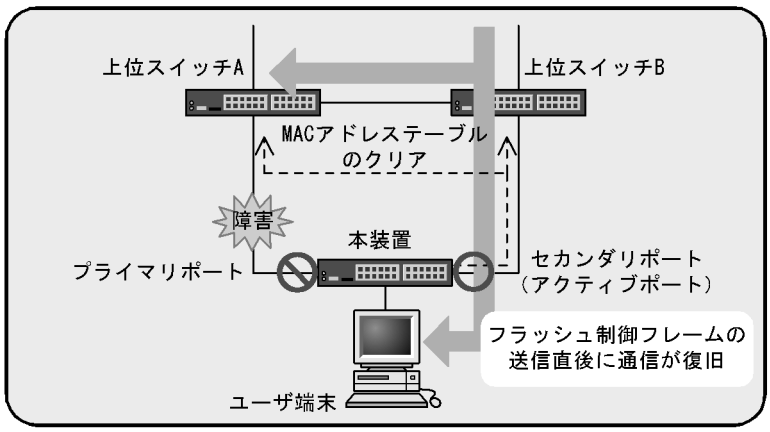


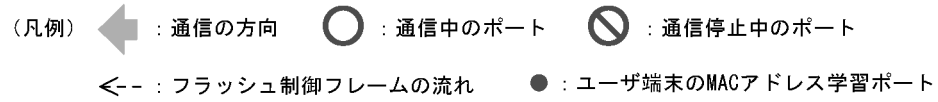
●障害時

フラッシュ制御フレームを送信しない場合



フラッシュ制御フレームを送信する場合





通常時

本装置のプライマリポートで通信を行っている状態では，上位スイッチはユーザ端末の MAC アドレスを，現在の通信経路で学習しています。

障害時（フラッシュ制御フレームの送信なし）
フラッシュ制御フレームを送信する設定がない場合，アクティブポートをセカンダリポートに切り替えても，上位スイッチ B がユーザ端末の MAC アドレスを以前のポートで学習しているため，上位スイッチ B が学習した MAC アドレスが消えるか，ユーザ端末からの通信がなければ，通信は復旧しません。

障害時（フラッシュ制御フレームの送信あり）
フラッシュ制御フレームを送信する設定の場合は，アクティブポートをセカンダリポートに切り替えると同時に，フラッシュ制御フレームによって上位スイッチ B が学習した MAC アドレスを削除するため，通信を速やかに復旧できます。

16.1.8 MAC アドレスアップデート機能

(1) 送信動作

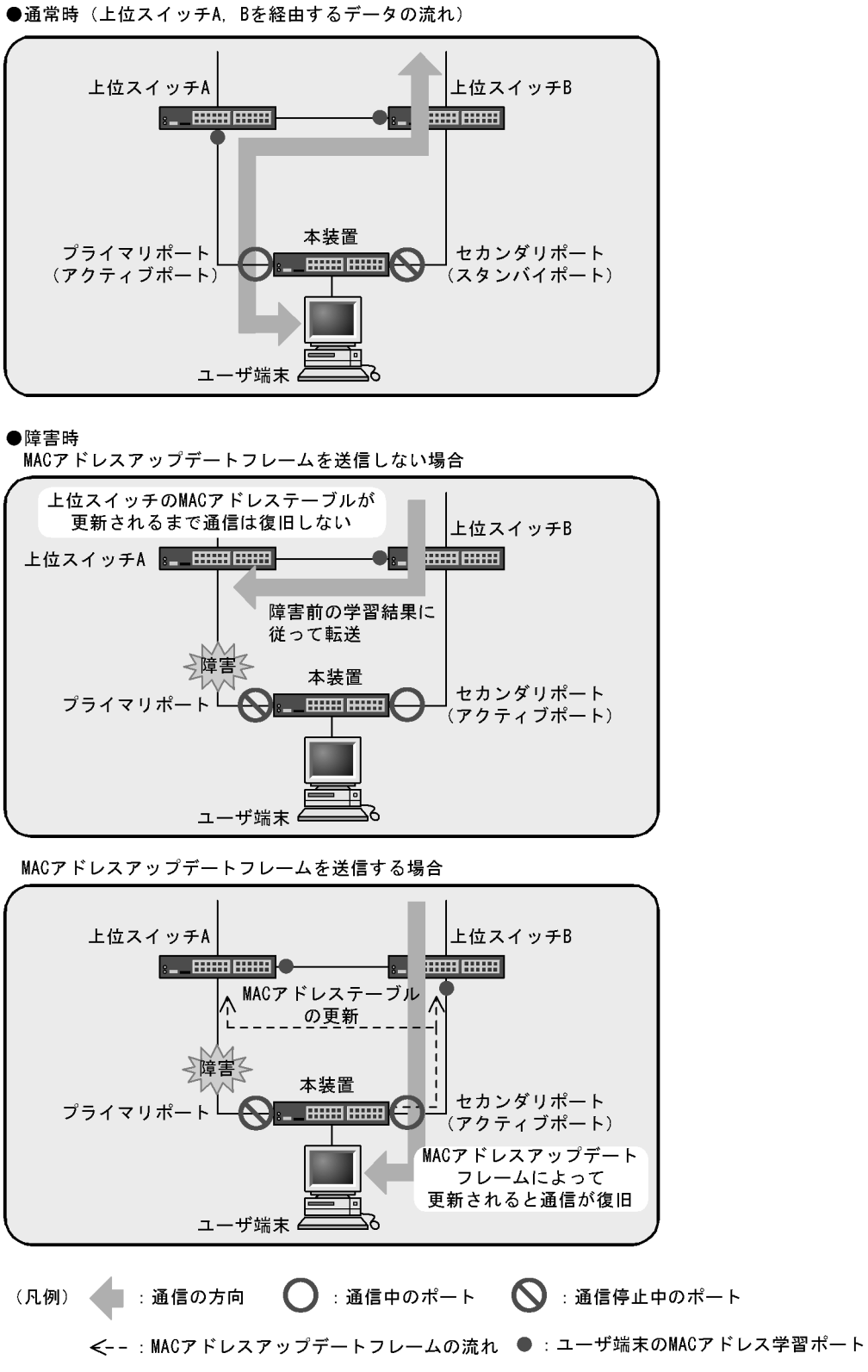
通信を行っているリンクの障害や運用コマンドによって，アクティブポートを変更した場合，通信を速やかに復旧させるために，上位スイッチに端末の MAC アドレスを再学習させる MAC アドレスアップデートフレームを送信できます。MAC アドレスアップデートフレームの特徴は次のとおりです。

- マルチキャストフレームである
- 送信元 MAC アドレスに，上位スイッチに再学習させる MAC アドレスを設定する
- 専用の受信機能を必要としない

MAC アドレスアップデート機能は，アップリンクポートごとに設定できます。また，送信対象外とする VLAN を指定できます。

MAC アドレスアップデートフレームの使用による切り替え動作の違いを次の図に示します。

図 16-5 MAC アドレスアップデートフレームの使用による切り替え動作の違い



通常時

本装置のプライマリポートで通信を行っている状態では，上位スイッチはユーザ端末の MAC アドレスを，現在の通信経路で学習しています。

障害時（MAC アドレスアップデートフレームの送信なし）

MAC アドレスアップデートフレームを送信する設定がない場合，アクティブポートをセカンダリポートに切り替えても，上位スイッチ B がユーザ端末の MAC アドレスを以前のポートで学習しているため，上位スイッチ B が学習した MAC アドレスが消えるか，ユーザ端末からの通信がなければ，通信は復旧しません。

障害時（MAC アドレスアップデートフレームの送信あり）

MAC アドレスアップデートフレームを送信する設定の場合は，アクティブポートをセカンダリポートに切り替えると同時に，MAC アドレスアップデートフレームによって上位スイッチ B がユーザ端末の MAC アドレス学習ポートを更新するため，通信を速やかに復旧できます。

MAC アドレスアップデート機能の仕様を次の表に示します。

表 16-2　MAC アドレスアップデート機能の仕様

項目	内容
送信対象ポートの設定単位	アップリンクポート単位
送信ポート	通信可能となったアクティブポート
送信回数※	1 ～ 3 回
送信対象となる MAC アドレスエントリ	次の二つの条件を同時に満たすエントリ • 該当のアップリンクポートが所属する VLAN で学習しているエントリ。ただし，コンフィグレーションで送信対象外に設定した VLAN で学習しているエントリは除きます。 • 該当のアップリンクポート以外で学習しているエントリ
送信対象となる MAC アドレスエントリ種別	• ダイナミックエントリ • スタティックエントリ • IEEE802.1X によるエントリ • Web 認証機能によるエントリ • MAC 認証機能によるエントリ • 装置 MAC アドレス • VLAN インタフェースの MAC アドレス • 仮想 MAC アドレス
最大送信 MAC アドレスエントリ	3000 エントリ。 送信対象のエントリが 3000 エントリを超えていた場合は，3000 エントリ分を送信するとともに，収容条件を超えていたことを示す運用ログを出力します。
送信レート	最大 300pps

注※

コンフィグレーションで設定できます。

(2) 受信動作

MAC アドレスアップデートフレームの中継時に，ほかの受信フレームと同様に送信元 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。詳細は，「コンフィグレーションガイド Vol.1　17. MAC アドレス学習」を参照してください。

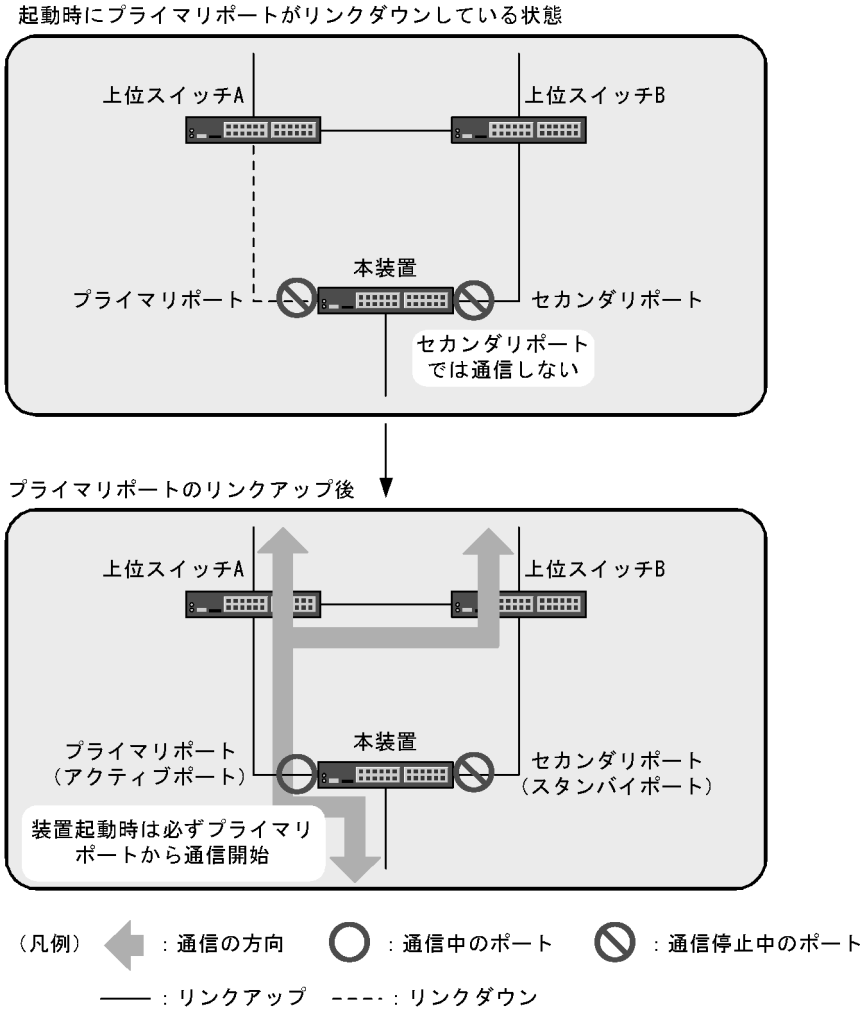
16.1.9　装置起動時のアクティブポート固定機能

装置起動時のアクティブポート固定機能は，本装置の起動時に，必ずプライマリポートから通信を開始したい場合に利用します。この機能を有効にした装置は，起動時にセカンダリポートがリンクアップしていても，プライマリポートがリンクアップするまではアップリンクポートでの通信をしません。

プライマリポートで通信を開始したあとは，通常と同じ動作となり，プライマリポートでの障害発生，または運用コマンドの実行によって，セカンダリポートでの通信に切り替わります。装置起動時にプライマリポート側の上位スイッチが故障しているなど，プライマリポートがリンクアップしない状態の場合には，運用コマンドの実行によって，セカンダリポートで通信を開始できます。

装置起動時のアクティブポート固定機能有効時の動作を次の図に示します。

図 16-6　装置起動時のアクティブポート固定機能有効時の動作



16.1.10　アップリンク・リダンダント使用時の注意事項

(1) 他機能との共存

アップリンク・リダンダントと，他機能との共存についての制限事項を次の表に示します。

表 16-3　他機能との共存

制限のある機能	制限の内容	備考
VLAN トンネリング	一部制限あり	アップリンクポートで使用できません。
Tag 変換	一部制限あり	
MAC アドレス学習	一部制限あり	スタティックエントリの設定は，アップリンクポートで使用できません。

制限のある機能	制限の内容	備考
スパニングツリー	共存不可	－
GSRP	共存不可	－
Ring Protocol	一部制限あり	リングポートで使用できません。
レイヤ 2 認証	一部制限あり	アップリンクポートで使用できません。

（凡例）－：なし

(2) フラッシュ制御フレーム送受信機能の使用について

上位スイッチで，アップリンク・リダンダントのフラッシュ制御フレーム受信機能をサポートしていることを確認してください。

上位スイッチが未サポートの場合，フラッシュ制御フレームを本装置から送信しても，MAC アドレステーブルがクリアされないため，通信の復旧までに時間が掛かることがあります。

(3) トランクポートでのフラッシュ制御フレーム送信設定について

トランクポートでフラッシュ制御フレームを送信する場合は，必ず送信先の VLAN を指定してください。VLAN の指定がない場合はネイティブ VLAN が存在するときだけ Untagged フレームのフラッシュ制御フレームを送信します。このとき，ネイティブ VLAN の設定がなければ，フラッシュ制御フレームは送信されません。

(4) 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

本装置にアップリンク・リダンダントに関するコンフィグレーションコマンドが設定されていない状態で，一つ目のアップリンク・リダンダントに関するコンフィグレーションコマンド（次に示すどれかのコマンド）を設定した場合に，すべての VLAN が一時的にダウンします。そのため，アップリンク・リダンダントを用いたネットワークを構築するときには，あらかじめ次に示すコンフィグレーションコマンドを設定しておくことを推奨します。

- switchport backup flush-request
- switchport backup interface
- switchport backup mac-address-table update exclude-vlan
- switchport backup mac-address-table update transmit

16.2 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

アップリンク・リダンダント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。

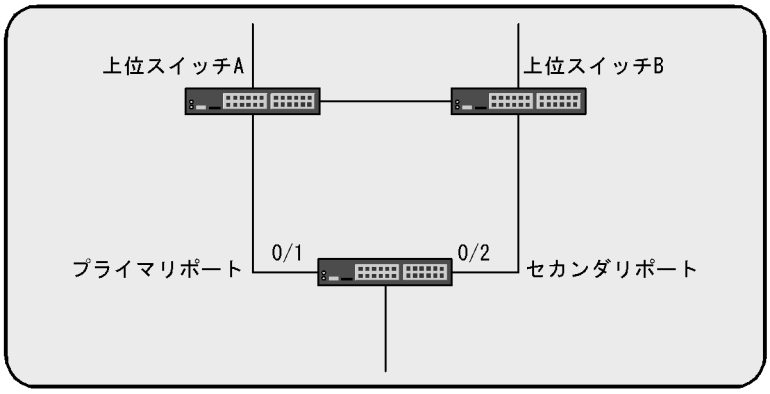
表 16-4 コンフィグレーションコマンド一覧

コマンド名	説明
switchport backup flush-request transmit	切り替えおよび切り戻し時に，上位スイッチに対して MAC アドレステーブルをクリアするためのフラッシュ制御フレームを送信する設定をします。
switchport backup interface	アップリンク・リダンダントのプライマリポートでセカンダリポートを指定し，アップリンクポートに設定します。また，自動切り戻し待ち時間を設定することで，自動切り戻しを有効にできます。
switchport backup mac-address-table update exclude-vlan	MAC アドレスアップデートフレームの送信時に送信対象外とする VLAN を設定します。
switchport backup mac-address-table update transmit	切り替えおよび切り戻し時に，上位スイッチに対して MAC アドレステーブルを更新するための MAC アドレスアップデートフレームを送信する設定をします。
switchport-backup startup-active-port-selection	装置起動時のアクティブポート固定機能の設定を有効にします。

16.2.2 アップリンク・リダンダントの設定

アップリンク・リダンダントの設定例を次の図に示します。ここでは，この図を基にアップリンク・リダンダントの設定手順を説明します。

図 16-7 アップリンク・リダンダントの設定例



本装置では，ポート 0/1 をプライマリポートに設定し，ポート 0/2 をセカンダリポートに設定します。また，自動切り戻しの待ち時間を 60 秒に設定し，フラッシュ制御フレームは送信する設定にします。

(1) アップリンク・リダンダントの設定

[設定のポイント]

ポート 0/1 をプライマリポート，ポート 0/2 をセカンダリポートとして設定し，自動切り戻しの待ち時間を 60 秒に設定します。アップリンク・リダンダントを設定するためには，事前にスパニングツリーを停止する必要があります。また，フラッシュ制御フレームを送信する設定は，プライマリポー

トで行う必要があります。

[コマンドによる設定]

1. **(config)# spanning-tree disable**
   スパニングツリーを停止します。

2. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport backup interface gigabitethernet 0/2 preemption-delay 60
   ポート 0/1 のコンフィグレーションモードへ移行します。
   プライマリポートになるポート 0/1 のコンフィグレーションモードで，セカンダリポートにするポート 0/2 を設定します。また，自動切り戻しの待ち時間を 60 秒に設定します。

3. **(config-if)# switchport backup flush-request transmit**
   (config-if)# exit
   フラッシュ制御フレームを送信する設定をします。

[注意事項]

- 本機能を設定する前は，ループ構成となります。プライマリポートまたはセカンダリポートのインタフェースを shutdown に設定するなどして，ループが発生しない状態にした上で，設定してください。
- プライマリポートをリンクアグリゲーションに設定する場合には，ポートチャネルインタフェースに設定してください。リンクアグリゲーションに設定されているポートのイーサネットインタフェースには設定できません。

16.3 オペレーション

16.3.1 運用コマンド一覧

アップリンク・リダンダントの運用コマンド一覧を次の表に示します。

表 16-5 運用コマンド一覧

コマンド名	説明
show switchport-backup	アップリンク・リダンダントの情報を表示します。
show switchport-backup statistics	アップリンク・リダンダントの統計情報を表示します。
clear switchport-backup statistics	アップリンク・リダンダントの統計情報を削除します。
set switchport-backup active	アクティブポートを変更する場合に，新しくアクティブポートになるポートを指定します。
restart uplink-redundant	アップリンク・リダンダントプログラムを再起動します。
dump protocols uplink-redundant	アップリンク・リダンダントのダンプ情報をファイルへ出力します。

16.3.2 アップリンク・リダンダント状態の表示

プライマリポートおよびセカンダリポートの状態や，フラッシュ制御フレームの送信先 VLAN を表示します。

図 16-8 show switchport-backup の実行結果

```
> show switchport-backup
Date 2009/09/04 16:48:07 UTC
startup active port selection: primary only
Switchport Backup pairs                          Preemption   Flush
 Primary    Status     Secondary  Status      Delay  Rest   VLAN  Update
 Port 0/1   Forwarding Port 0/24  Blocking        -     -   4094       -
 Port 0/10  Down       ChGr 4     Forwarding      -     -      -       1
*Port 0/11  Down       Port 0/15  Blocking        -     -     10       -
*Port 0/20  Down       Port 0/21  Down            -     -    200       -
>
```

- Status 表示
  通信しているアクティブポートは「Forwarding」，スタンバイポートは「Blocking」と表示されます。

16.3.3 アクティブポートの手動変更

set switchport-backup active コマンドで，アクティブポートを変更できます。

このコマンドは，指定したポートがスタンバイポートの場合だけ動作します。

図 16-9 set switchport-backup active の実行結果

```
> set switchport-backup active port 0/1
Are you sure to change the forwarding port to specified port? (y/n): y
>
```

17 IEEE802.3ah/UDLD

IEEE802.3ah/UDLD 機能は，片方向リンク障害を検出し，それに伴うネットワーク障害の発生を事前に防止する機能です。
この章では，IEEE802.3ah/UDLD 機能の解説と操作方法について説明します。

17.1　解説

17.1.1　概要

UDLD（Uni-Directional Link Detection）とは，片方向リンク障害を検出する機能です。

片方向リンク障害が発生すると，一方の装置では送信はできるが受信ができず，もう一方の装置では受信はできるが送信ができない状態になり，上位プロトコルで誤動作が発生し，ネットワーク上でさまざまな障害が発生します。よく知られている例として，スパニングツリーでのループ発生や，リンクアグリゲーションでのフレーム紛失が挙げられます。これらの障害は，片方向リンク障害を検出した場合に該当するポートを inactivate することによって未然に防ぐことができます。

IEEE802.3ah（Ethernet in the First Mile）で slow プロトコルの一部として位置づけられた OAM（Operations, Administration, and Maintenance）プロトコル（以下，IEEE802.3ah/OAM と示す）では，双方向リンク状態の監視を行うために，制御フレームを用いて定常的に対向装置と自装置の OAM 状態情報の交換を行い，相手装置とのフレームの到達性を確認する方式が述べられています。本装置では IEEE802.3ah/OAM 機能を用いて双方向リンク状態の監視を行い，その確認がとれない場合に片方向リンク障害を検出する方式で UDLD 機能を実現しています。

また，IEEE802.3ah/OAM プロトコルでは，Active モードと Passive モードの概念があり，Active モード側から制御フレームの送信が開始され，Passive モード側では，制御フレームを受信するまで制御フレームの送信は行いません。本装置では工場出荷時の設定で IEEE802.3ah/OAM 機能が有効になっていて，全ポートが Passive モードで動作します。

Ethernet ケーブルで接続された片方の装置側のポートにコンフィグレーションコマンド efmoam active udld を設定することで，片方向リンク障害の検出動作を行います。正しく片方向リンク障害を検出させるためには，もう一方の装置側のポートで IEEE802.3ah/OAM 機能が有効である必要があります。efmoam active udld コマンドを設定したポートで片方向リンク障害を検出した場合，該当するポートを inactivate することで対向装置側のポートでもリンクダウンが検出され，接続された双方の装置で該当ポートでの運用を停止します。

17.1.2　サポート仕様

IEEE802.3ah/UDLD 機能では，次の表に示すとおり IEEE802.3ah/OAM 機能をサポートしています。

表 17-1　IEEE802.3ah/UDLD でサポートする IEEE802.3ah OAMPDU

名称	説明	サポート
Information	相手装置に OAM 状態情報を送信する。	○
Event Notification	相手装置に Link Event の警告を送信する。	×
Variable Request	相手装置に MIB 変数を要求する。	×
Variable Response	要求された MIB 変数を送信する。	×
Loopback Control	相手装置の Loopback 状態を制御する。	×
Organization Specific	機能拡張用。	×

（凡例）○：サポート　×：未サポート

17.1.3 IEEE802.3ah/UDLD 使用時の注意事項

(1) IEEE802.3ah/UDLD 機能を設定した装置間に IEEE802.3ah/OAM 機能をサポートしない装置を接続した場合

一般的なスイッチでは，IEEE802.3ah/OAM 機能で使用する制御フレームは中継しません。このため，装置間で情報の交換ができず，コンフィグレーションコマンド efmoam active udld を設定したポートで片方向リンク障害を検出してしまいます。IEEE802.3ah/UDLD 機能の運用はできません。

(2) IEEE802.3ah/UDLD 機能を設定した装置間にメディアコンバータなどの中継装置を接続した場合

片方のリンク状態が切断された場合に，もう片方のリンク状態を自動的に切断しないメディアコンバータを装置間に設置した場合，装置間でリンク状態の認識にずれが生じます。このため，efmoam active udld コマンドを設定したポートで相手装置が動作していない状態でも片方向リンク障害を検出してしまいます。復旧する際にも，双方の装置で同期をとる必要があり，運用が困難になります。片方のリンク状態が切断された場合に，もう片方のリンク状態を自動的に切断する機能のあるメディアコンバータを使用してください。

(3) 他社の UDLD 機能との接続について

UDLD 機能はそれぞれ各社の独自仕様で機能を実装しているため，本装置の IEEE802.3ah/UDLD 機能と他社装置の UDLD 機能の相互接続はできません。

17.2 コンフィグレーション

17.2.1 コンフィグレーションコマンド一覧

IEEE802.3ah/UDLD のコンフィグレーションコマンド一覧を次の表に示します。

表 17-2 コンフィグレーションコマンド一覧

コマンド名	説明
efmoam active	物理ポートで IEEE802.3ah/OAM 機能の active モードにします。
efmoam disable	IEEE802.3ah/OAM 機能を無効にします。
efmoam udld-detection-count	片方向リンク障害とするためのカウンタ値を指定します。

17.2.2 IEEE802.3ah/UDLD の設定

(1) IEEE802.3ah/UDLD 機能の設定

[設定のポイント]

IEEE802.3ah/UDLD 機能を運用するには，先ず装置全体で IEEE802.3ah/OAM 機能を有効にしておくことが必要です。本装置では工場出荷時の設定で IEEE802.3ah/OAM 機能が有効となっている状態（全ポート Passive モード）です。次に，実際に片方向リンク障害検出機能を動作させたいポートに対し，UDLD パラメータを付加した Active モードの設定をします。

ここでは，gigabitethernet 0/1 で IEEE802.3ah/UDLD 機能を運用させます。

[コマンドによる設定]

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

   ポート 0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# efmoam active udld**

   ポート 0/1 で IEEE802.3ah/OAM 機能の Active モード動作を行い，片方向リンク障害検出動作を開始します。

(2) 片方向リンク障害検出カウントの設定

[設定のポイント]

片方向リンク障害は，相手からの情報がタイムアウトして双方向リンク状態の確認ができない状態が，決められた数だけ連続して発生した場合に検出します。この数が片方向リンク障害検出カウントです。双方向リンク状態は，1 秒に 1 回確認しています。

片方向リンク障害検出カウントを変更すると，実際に片方向リンク障害が発生してから検出するまでの時間を調整できます。片方向リンク障害検出カウントを少なくすると障害を早く検出する一方で，誤検出のおそれがあります。通常，本設定は変更する必要はありません。

片方向リンク障害発生から検出までのおよその時間を次に示します。なお，最大 10% の誤差が生じます。

5+（片方向リンク障害検出カウント）［秒］

[コマンドによる設定]

1. **(config)# efmoam udld-detection-count 60**

片方向リンク障害検出とするための相手からの情報タイムアウト発生連続回数を 60 回に設定します。

17.3 オペレーション

17.3.1 運用コマンド一覧

IEEE802.3ah/OAM 機能の運用コマンド一覧を次の表に示します。

表 17-3 運用コマンド一覧

コマンド名	説明
show efmoam	IEEE802.3ah/OAM の設定情報およびポートの設定情報を表示します。
show efmoam statistics	IEEE802.3ah/OAM に関する統計情報を表示します。
clear efmoam statistics	IEEE802.3ah/OAM に関する統計情報をクリアします。
restart efmoam	IEEE802.3ah/OAM プログラムを再起動します。
dump protocols efmoam	IEEE802.3ah/OAM プログラムで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

17.3.2 IEEE802.3ah/OAM 情報の表示

IEEE802.3ah/OAM 情報の表示は，運用コマンド show efmoam で行います。show efmoam コマンドは，IEEE802.3ah/OAM の設定情報と active モードに設定されたポートの情報を表示します。show efmoam detail コマンドは，active モードに設定されたポートに加え，相手装置を認識している passive モードのポートの情報を表示します。また，show efmoam statistics コマンドでは，IEEE802.3ah/OAM プロトコルの統計情報に加え，IEEE802.3ah/UDLD 機能で検出した障害状況を表示します。

図 17-1 show efmoam コマンドの実行結果

```
> show efmoam
Date 2006/10/02 23:59:59 UTC
Status: Enabled
udld-detection-count: 30
Port   Link status     UDLD status    Dest MAC
0/1    Up              detection    * 0012.e298.dc20
0/2    Down            active         unknown
0/4    Down(uni-link)  detection      unknown
>
```

図 17-2 show efmoam detail コマンドの実行結果

```
> show efmoam detail
Date 2006/10/02 23:59:59 UTC
Status: Enabled
udld-detection-count: 30
Port   Link status     UDLD status    Dest MAC
0/1    Up              detection    * 0012.e298.dc20
0/2    Down            active         unknown
0/3    Up              passive        0012.e298.7478
0/4    Down(uni-link)  detection      unknown
>
```

図 17-3 show efmoam statistics **コマンドの実行結果**

```
> show efmoam statistics
Date 2006/10/02 23:59:59 UTC
Port 0/1 [detection]
  OAMPDUs   :Tx       =       295  Rx       =       295
             Invalid  =         0  Unrecogn.=         0
  TLVs      :Invalid  =         0  Unrecogn.=         0
  Info TLV  :Tx_Local =       190  Tx_Remote=       105  Rx_Remote=       187
             Timeout  =         3  Invalid  =         0  Unstable =         0
  Inactivate:TLV      =         0  Timeout  =         0
Port 0/2 [active]
  OAMPDUs   :Tx       =       100  Rx       =       100
             Invalid  =         0  Unrecogn.=         0
  TLVs      :Invalid  =         0  Unrecogn.=         0
  Info TLV  :Tx_Local =       100  Tx_Remote=       100  Rx_Remote=       100
             Timeout  =         0  Invalid  =         0  Unstable =         0
  Inactivate:TLV      =         0  Timeout  =         0
Port 0/3 [passive]
  OAMPDUs   :Tx       =       100  Rx       =       100
             Invalid  =         0  Unrecogn.=         0
  TLVs      :Invalid  =         0  Unrecogn.=         0
  Info TLV  :Tx_Local =         0  Tx_Remote=       100  Rx_Remote=       100
             Timeout  =         0  Invalid  =         0  Unstable =         0
  Inactivate:TLV      =         0  Timeout  =         0
>
```

18 ストームコントロール

ストームコントロールはフラッディング対象フレーム中継の量を制限する機能です。この章では，ストームコントロールの解説と操作方法について説明します。

18.1 解説

18.1.1 ストームコントロールの概要

レイヤ2ネットワークでは，ネットワーク内にループが存在すると，ブロードキャストフレームなどがスイッチ間で無制限に中継されて，ネットワークおよび接続された機器に異常な負荷を掛けることになります。このような現象はブロードキャストストームと呼ばれ，レイヤ2ネットワークでは避けなければならない問題です。マルチキャストフレームが無制限に中継されるマルチキャストストーム，ユニキャストフレームが無制限に中継されるユニキャストストームも防止する必要があります。

ネットワークおよび接続された機器への影響を抑えるために，スイッチでフラッディング対象フレーム中継の量を制限する機能がストームコントロールです。

本装置では，イーサネットインタフェースごとに，閾値として1秒間で受信する最大フレーム数を設定でき，その値を超えたフレームを廃棄します。閾値の設定は，ブロードキャストフレーム，マルチキャストフレーム，ユニキャストフレームの3種類のフレームで個別に設定します。

さらに，受信したフレーム数が閾値を超えた場合，そのポートを閉塞したり，プライベートトラップやログメッセージを出力できます。

ストームコントロールの運用コマンドはありません。

18.1.2 ストームコントロール使用時の注意事項

(1) ユニキャストフレームの扱い

本装置では，ユニキャストストームの検出と，フレームの廃棄で対象フレームが異なります。ユニキャストストームの検出は，受信するすべてのユニキャストフレームの数で行います。フレームの廃棄は，MACアドレステーブルに宛先MACアドレスが登録されていないためにフラッディングされるユニキャストフレームだけが対象です。

(2) ストームの検出と回復の検出

本装置は，1秒間に受信したフレーム数が，コンフィグレーションで設定された閾値を超えたときに，ストームが発生したと判定します。ストームが発生したあと，1秒間に受信したフレーム数が閾値以下の状態が30秒続いたときに，ストームが回復したと判定します。

ストーム発生時にポートを閉塞する場合は，そのポートではフレームを受信しなくなるため，ストームの回復も検出できなくなります。ストーム発生時にポートの閉塞を設定した場合は，ネットワーク監視装置などの本装置とは別の手段でストームが回復したことを確認してください。

18.2 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

ストームコントロール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 18-1 コンフィグレーションコマンド一覧

コマンド名	説明
storm-control	ストームコントロールの閾値を設定します。また，ストームを検出した場合の動作を設定できます。

18.2.2 ストームコントロールの設定

● ブロードキャストフレームの抑制

ブロードキャストストームを防止するためには，イーサネットインタフェースで受信するブロードキャストフレーム数を閾値として設定します。ブロードキャストフレームには，ARP パケットなど通信に必要なフレームも含まれるので，閾値には通常使用するフレーム数を考慮して余裕のある値を設定します。

● マルチキャストフレームの抑制

マルチキャストストームを防止するためには，イーサネットインタフェースで受信するマルチキャストフレーム数を閾値として設定します。マルチキャストフレームには，IPv4 マルチキャストパケット，IPv6 マルチキャストパケット，OSPF パケットなどの制御パケットなど通信に必要なフレームも含まれるので，閾値には通常使用するフレーム数を考慮して余裕のある値を設定します。

● ユニキャストストームの抑制

ユニキャストストームを防止するためには，イーサネットインタフェースで受信するユニキャストフレーム数を閾値として設定します。閾値には通常使用するフレーム数を考慮して余裕のある値を設定します。

なお，本装置では，ユニキャストフレームの検出には，受信する全ユニキャストフレーム数を使用しますが，中継せずに廃棄するフレームは，MAC アドレステーブルに宛先 MAC アドレスが登録されていないためにフラッディングされるユニキャストフレームだけが対象です。特にストーム検出時の動作にポートの閉塞を指定する場合は，通常使用するフレームでストーム検出とならないよう，閾値の設定には十分余裕のある値としてください。

● ストーム検出時の動作

ストームを検出したときの本装置の動作を設定します。ポートの閉塞，プライベートトラップの送信，ログメッセージの出力を，ポートごとに組み合わせて選択できます。

- ポートの閉塞
  ストームを検出したとき，そのポートを inactive 状態にします。ストームが回復したあと，再びそのポートを active 状態に戻すには，activate コマンドを使用します。
- プライベートトラップの送信
  ストームを検出したときおよびストームの回復を検出したとき，プライベートトラップを送信して通知します。
- ログメッセージの出力
  ストームを検出したときおよびストームの回復を検出したとき，ログメッセージを出力して通知します。ただし，ポートの閉塞時のメッセージは必ず出力します。

[設定のポイント]

設定できるインタフェースはイーサネットインタフェースです。

ストームが発生したとき，ポートを閉塞します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/10**
   (config-if)# storm-control broadcast level pps 50
   ブロードキャストフレームの閾値を 50 に設定します。

2. **(config-if)# storm-control mutlicast level pps 500**
   マルチキャストフレームの閾値を 500 に設定します。

3. **(config-if)# storm-control unicast level pps 1000**
   ユニキャストフレームの閾値を 1000 に設定します。

4. **(config-if)# storm-control action inactivate**
   ストームを検出したときに，ポートを inactive 状態にします。

19 L2 ループ検知

L2 ループ検知機能は，レイヤ 2 ネットワークでループ障害を検知し，ループの原因となるポートを inactive 状態にすることでループ障害を解消する機能です。
この章では，L2 ループ検知機能の解説と操作方法について説明します。

19.1 解説

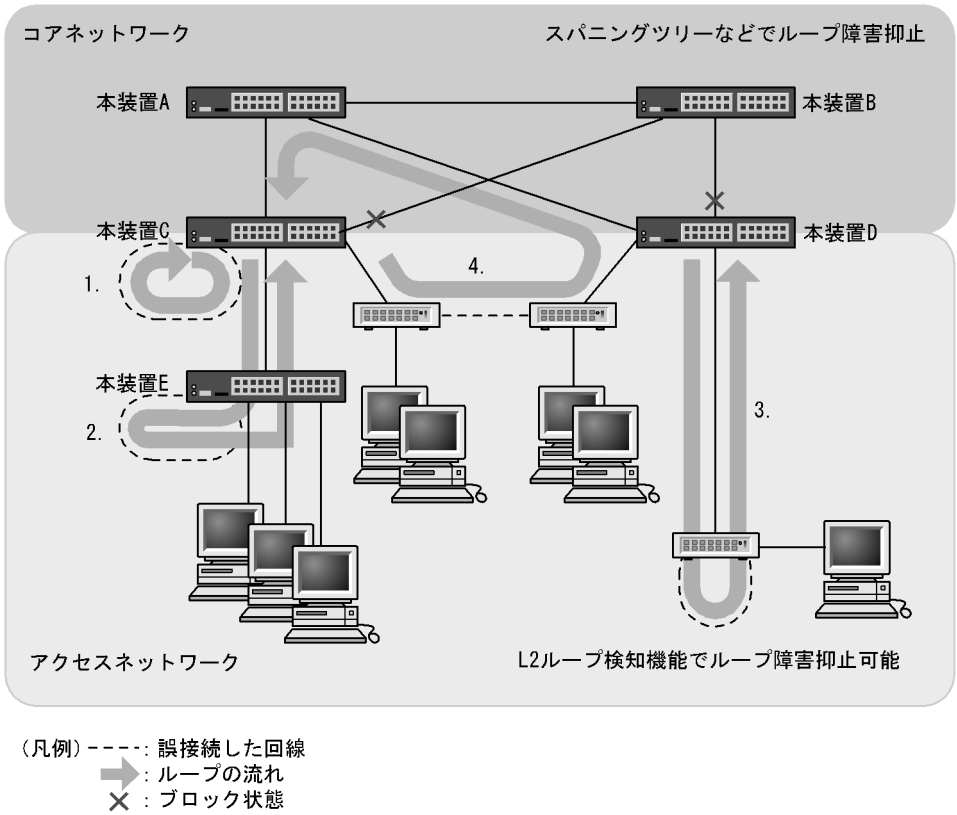
19.1.1 概要

レイヤ 2 ネットワークでは，ネットワーク内にループ障害が発生すると，MAC アドレス学習が安定しなくなったり，装置に負荷が掛かったりして正常な通信ができない状態になります。このような状態を回避するためのプロトコルとして，スパニングツリーや Ring Protocol などがありますが，L2 ループ検知機能は，一般的にそれらプロトコルを動作させているコアネットワークではなく，冗長化をしていないアクセスネットワークでのループ障害を解消する機能です。

L2 ループ検知機能は，自装置でループ障害を検知した場合，検知したポートを inactive 状態にすることで，原因となっている個所をネットワークから切り離し，ネットワーク全体にループ障害が波及しないようにします。

ループ障害の基本パターンを次の図に示します。

図 19-1 ループ障害の基本パターン



ループ障害のパターン例

1. 自装置で回線を誤接続し，ループ障害が発生している。
2，3. 自装置から下位の本装置または L2 スイッチで回線を誤接続し，ループ障害が発生している。
4. 下位装置で回線を誤接続し，コアネットワークにわたるループ障害が発生している。

L2 ループ検知機能は，このような自装置での誤接続や他装置での誤接続など，さまざまな場所でのループ障害を検知できます。

19.1.2 動作仕様

L2 ループ検知機能では，コンフィグレーションで設定したポート（物理ポートまたはチャネルグループ）から L2 ループ検知用の L2 制御フレーム（L2 ループ検知フレーム）を定期的に送信します。L2 ループ検知機能が有効なポートでその L2 ループ検知フレームを受信した場合，ループ障害と判断し，受信したポートまたは送信元ポートを inactive 状態にします。

inactive 状態のポートは，ループ障害の原因を解決後に運用コマンドで active 状態にします。また，自動復旧機能を設定しておけば，自動的に active 状態にできます。

(1) L2 ループ検知機能のポート種別

L2 ループ検知機能で使用するポートの種別を次の表に示します。

表 19-1 ポート種別

種別	機能
検知送信閉塞ポート	• ループを検知するための L2 ループ検知フレームを送信します。 • ループ障害検知時は，運用ログを表示し，当該ポートを inactive 状態にします。
検知送信ポート	• ループを検知するための L2 ループ検知フレームを送信します。 • ループ障害検知時は，運用ログを表示します。inactive 状態にはしません。
検知ポート （コンフィグレーション省略時）	• ループを検知するための L2 ループ検知フレームは送信しません。 • ループ障害検知時は，運用ログを表示します。inactive 状態にはしません。
検知対象外ポート	• 本機能の対象外ポートです。ループを検知するための L2 ループ検知フレームの送信やループ障害検知をしません。
アップリンクポート	• ループを検知するための L2 ループ検知フレームは送信しません。 • ループ障害検知時は，送信元ポートで，送信元のポート種別に従った動作をします。例えば，送信元が検知送信閉塞ポートであれば，運用ログを表示し，送信元ポートを inactive 状態にします。

(2) L2 ループ検知フレームの送信ポートについて

L2 ループ検知フレームは，検知送信閉塞ポートと検知送信ポートに所属しているすべての VLAN から，設定した送信間隔で送信します。本機能で送信できる最大フレーム数は決まっていて，それを超えるフレームは送信しません。フレームを送信できなかったポートや VLAN では，ループ障害を検知できなくなります。そのため，送信できる最大フレーム数は，収容条件に従って設定してください。詳細については，マニュアル「コンフィグレーションガイド Vol.1　3. 収容条件」を参照してください。

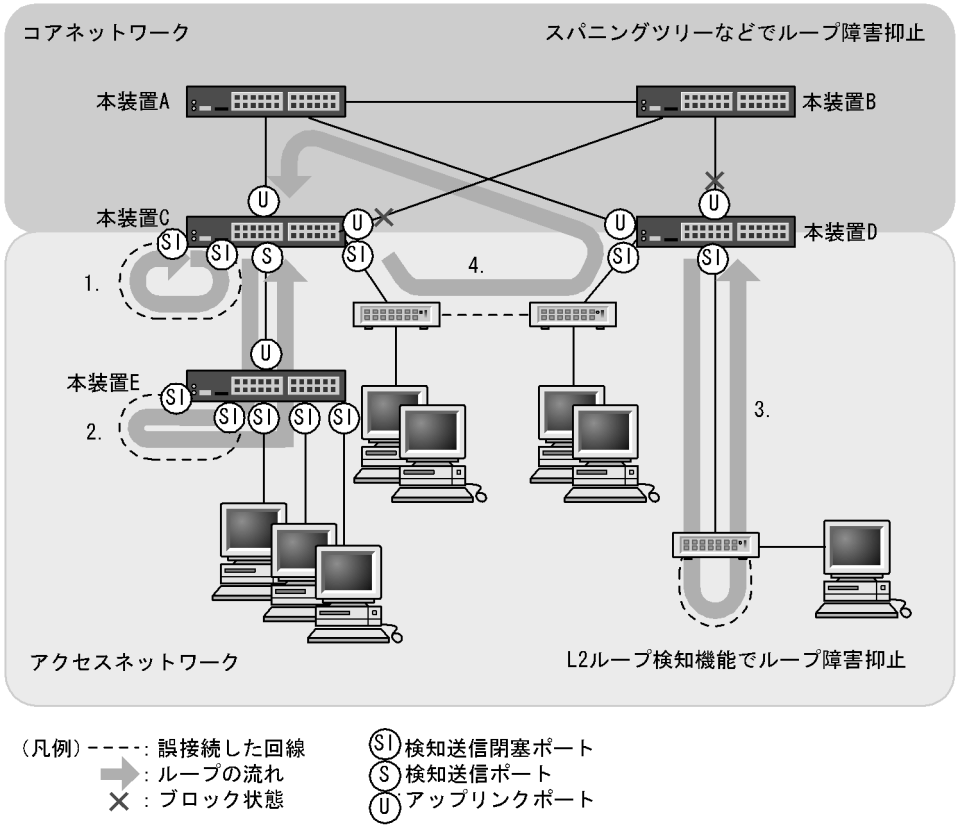
(3) ループ障害の検知方法とポートを inactive 状態にする条件

自装置から送信した L2 ループ検知フレームを受信した場合，ポートごとに受信数を計上し，コンフィグレーションで設定した L2 ループ検知フレーム受信数（初期値は 1）に達すると，該当するポートを inactive 状態（検知送信閉塞ポートだけ）にします。

19.1.3 適用例

L2 ループ検知機能を適用したネットワーク構成を示します。

図 19-2 L2 ループ検知機能を適用したネットワーク構成



(1) 検知送信閉塞ポートの適用

L2 ループ検知機能で一般的に設定するポート種別です。本装置 C，D，E で示すように，下位側のポートに設定しておくことで，1，2，3 のような下位側の誤接続によるループ障害に対応します。

(2) 検知送信ポートの適用

ループ障害の波及範囲を局所化するためには，できるだけ下位の装置で本機能を動作させるほうが有効です。本装置 C と本装置 E のように多段で接続している場合に，2. のような誤接続で本装置 C 側のポートを inactive 状態にすると，本装置 E のループ障害と関係しないすべての端末で上位ネットワークへの接続ができなくなります。そのため，より下流となる本装置 E で L2 ループ検知機能を動作させることを推奨します。

なお，その場合は，本装置 C 側のポートには検知送信ポートを設定しておきます。この設定によって，正常運用時は本装置 E でループ障害を検知しますが，本装置 E で L2 ループ検知機能の設定誤りなどでループ障害を検知できないときには，本装置 C でループ障害を検知（inactive 状態にはならない）できます。

(3) アップリンクポートの適用

上位ネットワークに繋がっているポートまたはコアネットワークに接続するポートで設定します。この設定によって，4. のような誤接続となった場合，装置 C の送信元ポートが inactive 状態になるため，コアネットワークへの接続を確保できます。

19.1.4 L2 ループ検知使用時の注意事項

(1) プロトコル VLAN や MAC VLAN での動作について

L2 ループ検知フレームは，独自フォーマットの Untagged フレームです。プロトコルポートや MAC ポートではネイティブ VLAN として転送されるため，次に示す条件をどちらも満たしている場合，装置間にわたるループ障害が検知できないおそれがあります。

- コアネットワーク側のポートをアップリンクポートとして設定している
- コアネットワーク側にネイティブ VLAN を設定していない

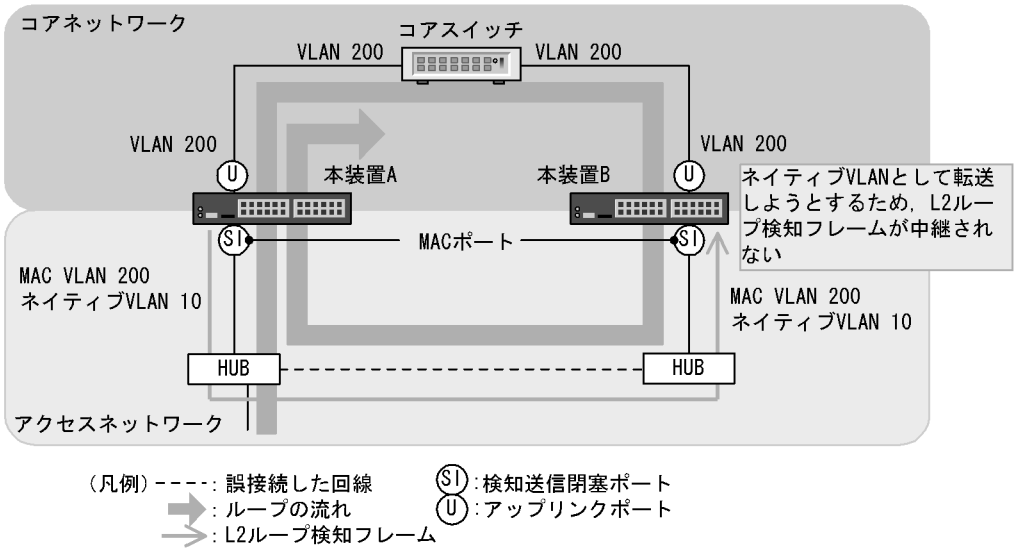
この場合は，アップリンクポートとして設定しているコアネットワーク側のポートを検知送信ポートに設定すると，ループ障害を検知できます。具体的な構成例を次に示します。

(a) ループ検知の制限となる構成例

次の図に示す構成で本装置配下の HUB 間を誤接続すると，装置間にわたるループが発生します。

本装置 A は HUB 側の検知送信閉塞ポートから L2 ループ検知フレームを送信し，コアスイッチ側のアップリンクポートからは送信しません。本装置 B は MAC ポートで受信した L2 ループ検知フレームをネイティブ VLAN として転送しようとするため，L2 ループ検知フレームはコアスイッチ側へ中継されません。この場合，L2 ループ検知フレームは本装置 A へ戻ってこないため，ループ障害を検知できません。

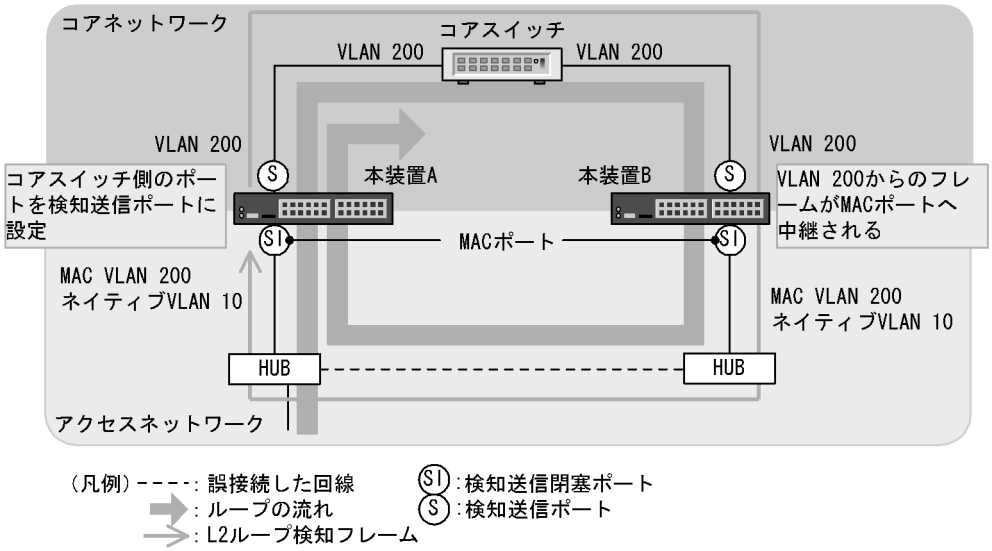
図 19-3 ループ検知の制限となる構成



(b) ループ検知可能な構成例

本装置 A のコアスイッチ側のポートを検知送信ポートに設定した場合，本装置 B はコアスイッチ側のポートから受信した L2 ループ検知フレームを MAC ポートへ中継するため，本装置 A でループ障害が検知できます。

図 19-4 ループ検知可能な構成



（2） Tag 変換機能使用時の動作について

本装置の Tag 変換ポートから送信した L2 ループ検知フレームを Tag 変換後の VLAN で受信した場合，ループ障害と判断します。また，他装置で Tag 変換されて本装置の別の VLAN として L2 ループ検知フレームを受信した場合もループ障害と判断します。

（3） L2 ループ検知機能の動作環境について

本機能を使用する場合に，同一ネットワーク内に L2 ループ検知未サポートの AX6700S，AX6300S 装置（Ver.10.7 より前）を配置したとき，その装置でループ検知フレームを受信するとフレームを廃棄します。そのため，その装置を含む経路でループ障害が発生しても検知できません。

（4） inactive 状態にしたポートを自動的に active 状態にする機能（自動復旧機能）について

スタティックリンクアグリゲーション上で自動復旧機能を使用する場合は，次の点に注意してください。

- 回線速度を変更（ネットワーク構成の変更）する場合は，該当チャネルグループに異速度混在モードを設定してください。異速度混在モードを設定しないで回線速度を変更中にループを検知した場合，該当チャネルグループで自動復旧機能が動作しないおそれがあります。
- オートネゴシエーションで接続する場合は回線速度を指定してください。指定しないと，回線品質の劣化などによって一時的に回線速度が異なる状態になり，低速回線が該当チャネルグループから離脱することがあります。この状態でループを検知した場合，該当チャネルグループで自動復旧機能が動作しないおそれがあります。

自動復旧機能が動作しない場合は，ループ原因を解消したあと，運用コマンド activate でポートを active 状態にしてください。

19.2 コンフィグレーション

19.2.1 コンフィグレーションコマンド一覧

L2 ループ検知のコンフィグレーションコマンド一覧を次の表に示します。

表 19-2 コンフィグレーションコマンド一覧

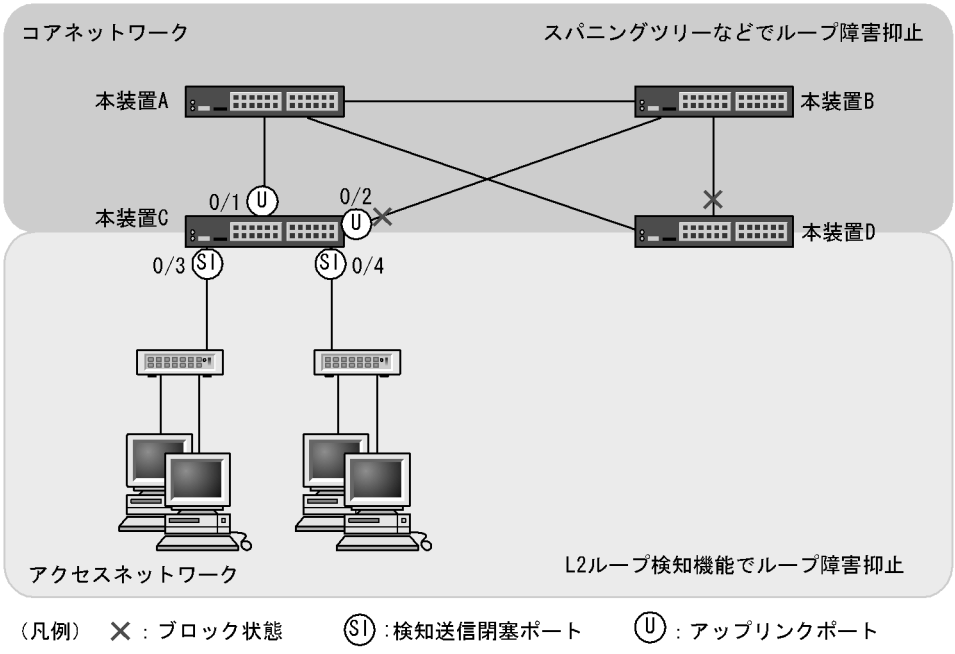
コマンド名	説明
loop-detection	L2 ループ検知機能でのポート種別を設定します。
loop-detection auto-restore-time	inactive 状態にしたポートを自動的に active 状態にするまでの時間を秒単位で指定します。
loop-detection enable	L2 ループ検知機能を有効にします。
loop-detection hold-time	inactive 状態にするまでの L2 ループ検知フレーム受信数の保持時間を秒単位で指定します。
loop-detection interval-time	L2 ループ検知フレームの送信間隔を設定します。
loop-detection threshold	ポートを inactive 状態にするまでの L2 ループ検知フレーム受信数を設定します。

19.2.2 L2 ループ検知の設定

L2 ループ検知機能を設定する手順を次に示します。ここでは，次の図に示す本装置 C の設定例を示します。

ポート 0/1 および 0/2 はコアネットワークと接続しているため，アップリンクポートを設定します。ポート 0/3 および 0/4 は下位装置と接続しているため，検知送信閉塞ポートを設定します。

図 19-5 L2 ループ検知の設定例



(1) L2 ループ検知機能の設定

[設定のポイント]

L2 ループ検知機能のコンフィグレーションでは，装置全体で機能を有効にする設定と，実際に L2 ループ障害を検知したいポートを設定する必要があります。

[コマンドによる設定]

1. **(config)# loop-detection enable**
   本装置で L2 ループ検知機能を有効にします。

2. **(config)# interface range gigabitethernet 0/1-2**
   (config-if-range)# loop-detection uplink-port
   (config-if-range)# exit
   ポート 0/1 および 0/2 をアップリンクポートに設定します。この設定によって，ポート 0/1 および 0/2 で L2 ループ検知フレームを受信した場合，送信元ポートに対して送信元のポート種別に従った動作をします。

3. **(config)# interface range gigabitethernet 0/3-4**
   (config-if-range)# loop-detection send-inact-port
   (config-if-range)# exit
   ポート 0/3 および 0/4 を検知送信閉塞ポートに設定します。この設定によって，ポート 0/3 および 0/4 で L2 ループ検知フレームを送信し，また，本ポートでループ障害検知時は，本ポートを inactive 状態にします。

(2) L2 ループ検知フレームの送信間隔の設定

[設定のポイント]

L2 ループ検知フレームの最大送信レートを超えたフレームは送信しません。フレームを送信できなかったポートや VLAN では，ループ障害を検知できなくなります。L2 ループ検知フレームの最大送信レートを超える場合は，送信間隔を長く設定し最大送信レートに収まるようにする必要があります。

[コマンドによる設定]

1. **(config)# loop-detection interval-time 60**
   L2 ループ検知フレームの送信間隔を 60 秒に設定します。

(3) inactive 状態にする条件の設定

[設定のポイント]

通常は，1 回のループ障害の検知で inactive 状態にします。この場合，初期値（1 回）のままで運用できます。しかし，瞬間的なループで inactive 状態にしたくない場合には，inactive 状態にするまでの L2 ループ検知フレーム受信数を設定できます。

[コマンドによる設定]

1. **(config)# loop-detection threshold 100**
   L2 ループ検知フレームを 100 回受信することで inactive 状態にするように設定します。

2. **(config)# loop-detection hold-time 60**

L2 ループ検知フレームを最後に受信してからの受信数を 60 秒保持するように設定します。

(4) 自動復旧時間の設定

[設定のポイント]

inactive 状態にしたポートを自動的に active 状態にしたい場合に設定します。

[コマンドによる設定]

1. **(config)# loop-detection auto-restore-time 300**
   300 秒後に，inactive 状態にしたポートを自動的に active 状態に戻す設定をします。

19.3 オペレーション

19.3.1 運用コマンド一覧

L2 ループ検知の運用コマンド一覧を次の表に示します。

表 19-3 運用コマンド一覧

コマンド名	説明
show loop-detection	L2 ループ検知情報を表示します。
show loop-detection statistics	L2 ループ検知の統計情報を表示します。
show loop-detection logging	L2 ループ検知のログ情報を表示します。
clear loop-detection statistics	L2 ループ検知の統計情報をクリアします。
clear loop-detection logging	L2 ループ検知のログ情報をクリアします。
restart loop-detection	L2 ループ検知プログラムを再起動します。
dump protocols loop-detection	L2 ループ検知のダンプ情報をファイルへ出力します。

19.3.2 L2 ループ状態の確認

show loop-detection コマンドで L2 ループ検知の設定と運用状態を確認できます。

L2 ループ検知フレームの送信レートが最大値を超えて，フレームを送信できないポートがないかを確認できます。VLAN Port Counts の Configuration が Capacity を超えていない場合は問題ありません。

ループ障害によって inactive 状態となっているポートは Port Information の Status で確認できます。

図 19-6 L2 ループ検知の情報

```
> show loop-detection
Date 2008/04/21 12:10:10 UTC
Interval Time           :10
Output Rate             :30pps
Threshold               :1
Hold Time               :infinity
Auto Restore Time       :-
VLAN Port Counts
    Configuration       :103          Capacity       :300
Port Information
  Port   Status      Type         DetectCnt RestoringTimer  SourcePort  Vlan
  0/1    Up          send-inact           0              -  -
  0/2    Down        send-inact           0              -  -
  0/3    Up          send                 0              -  -
  0/4    Up          exception            0              -  -
  0/5    Down(loop)  send-inact           1              -  CH:32(U)     100
  CH:1   Up          trap                 0              -  -
  CH:32  Up          uplink               -              -  0/5          100
>
```

20 CFM

CFM（Connectivity Fault Management）は，レイヤ 2 レベルでのブリッジ間の接続性の検証とルート確認を行う，広域イーサネット網の保守管理機能です。
この章では，CFM の解説と操作方法について説明します。

20.1 解説

20.1.1 概要

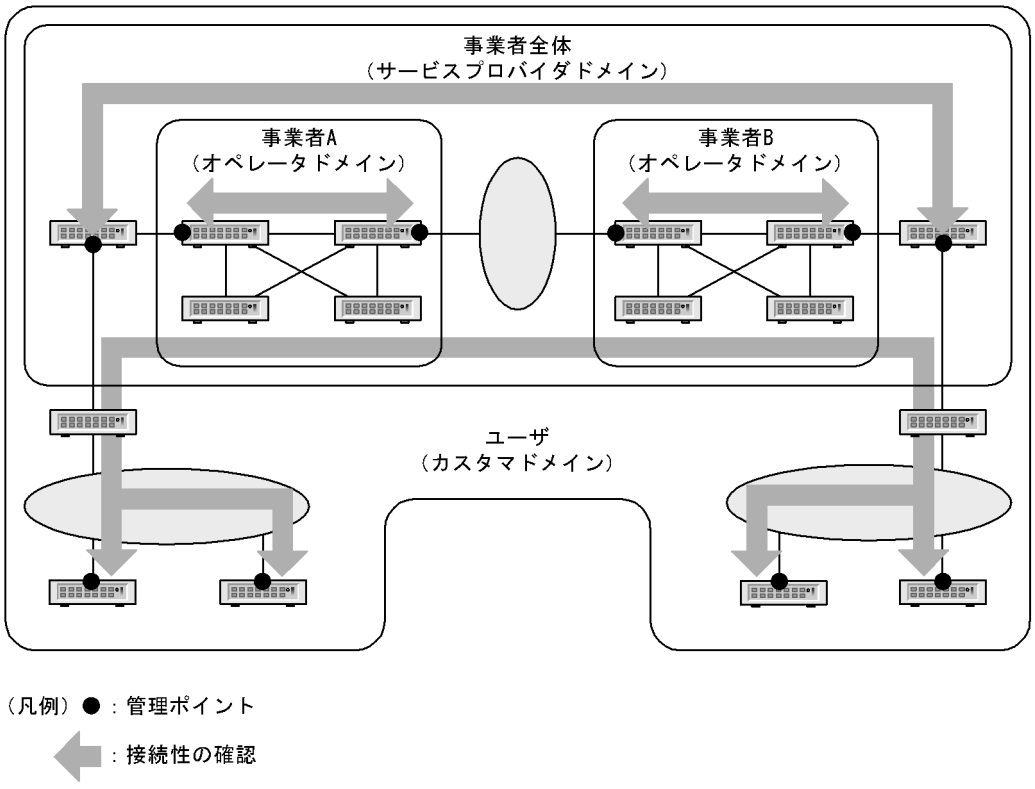
イーサネットは企業内 LAN だけでなく広域網でも使われるようになってきました。これに伴い，イーサネットに SONET や ATM と同等の保守管理機能が求められています。

CFM では，次の三つの機能を使って，レイヤ 2 ネットワークの保守管理を行います。

1. Continuity Check
   管理ポイント間で，情報が正しく相手に届くか（到達性・接続性）を常時監視します。
2. Loopback
   障害を検出したあと，Loopback でルート上のどこまで到達するのかを特定します（ループバック試験）。
3. Linktrace
   障害を検出したあと，Linktrace で管理ポイントまでのルートを確認します（レイヤ 2 ネットワーク内のルート探索）。

CFM の構成例を次の図に示します。

図 20-1 CFM の構成例



(1) CFM の機能

CFM は IEEE802.1ag で規定されていて，次の表に示す機能があります。本装置は，これらの機能をサポートしています。

表 20-1 CFM の機能

名称	説明
Continuity Check（CC）	管理ポイント間の到達性の常時監視
Loopback	ループバック試験 ping 相当の機能をレイヤ 2 で実行します。
Linktrace	ルート探索 traceroute 相当の機能をレイヤ 2 で実行します。

(2) CFM の構成

CFM を構成する要素を次の表に示します。CFM はドメイン，MA，MEP および MIP から構成された保守管理範囲内で動作します。

表 20-2 CFM を構成する要素

名称	説明
ドメイン （Maintenance Domain）	CFM を適用するネットワーク上の管理用のグループのこと。
MA （Maintenance Association）	ドメインを細分化して管理する VLAN のグループのこと。
MEP （Maintenance association End Point）	管理終端ポイントのこと。 ドメインの境界上のポートで，MA 単位に設定します。 また，CFM の各機能を実行するポートです。
MIP （Maintenance domain Intermediate Point）	管理中間ポイントのこと。 ドメインの内部に位置する管理ポイントです。
MP （Maintenance Point）	管理ポイントのことで，MEP と MIP の総称です。

20.1.2 CFM の構成要素

(1) ドメイン

CFM ではドメインという単位でネットワークを階層的に管理し，ドメイン内で CFM PDU を送受信することで保守管理を行います。ドメインには 0 ～ 7 のレベル（ドメインレベル）があり，レベルの値が大きいほうが高いレベルとなります。

高いドメインレベルでは，低いドメインレベルの CFM PDU を廃棄します。低いドメインレベルでは，高いドメインレベルの CFM PDU を処理しないで転送します。したがって，低いドメインレベルの CFM PDU が高いドメインレベルのドメインに渡ることはなく，ドメインで独立した保守管理ができます。

ドメインレベルは区分に応じて使用するように，規格で規定されています。区分に割り当てられたドメインレベルを次の表に示します。

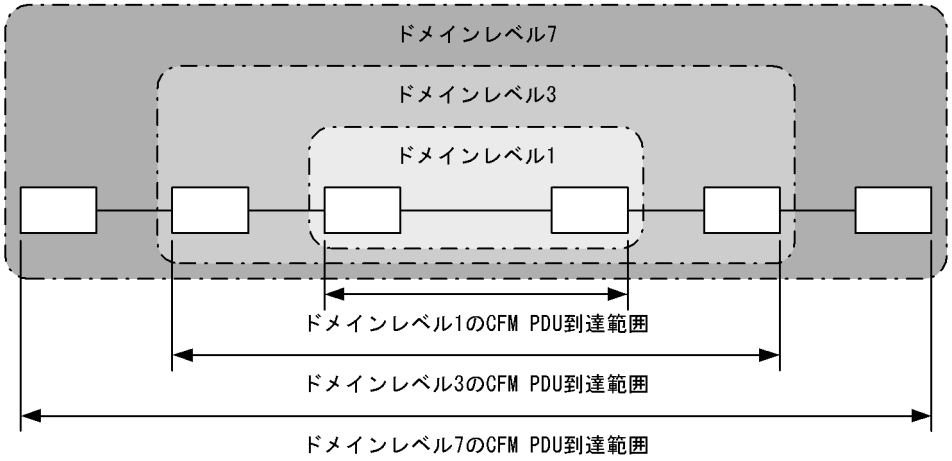
表 20-3 区分に割り当てられたドメインレベル

ドメインレベル	区分
7	カスタマ（ユーザ）
6	
5	
4	サービスプロバイダ（事業者全体）

ドメインレベル	区分
3	
2	オペレータ（事業者）
1	
0	

ドメインは階層的に設定できます。ドメインを階層構造にする場合は低いドメインレベルを内側に，高いドメインレベルを外側に設定します。階層的なドメインの構成例を次の図に示します。

図 20-2　階層的なドメインの構成例



(2) MA

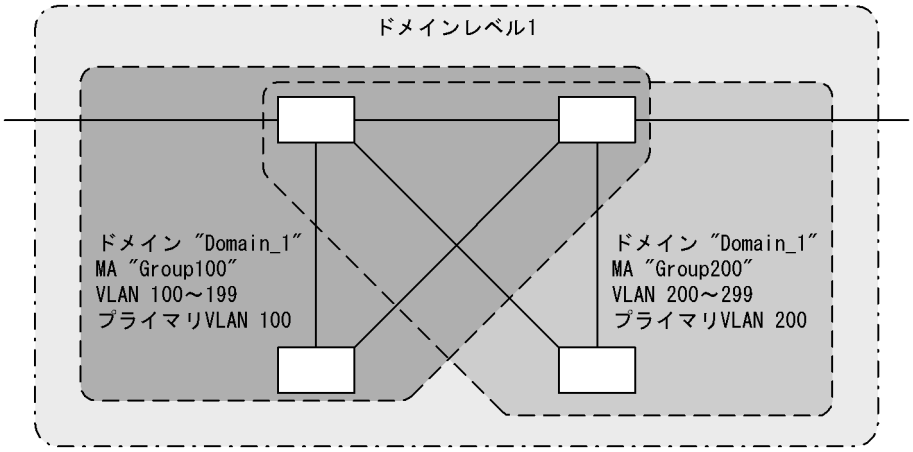
MA はドメイン内を VLAN グループで分割して管理する場合に使います。ドメインには最低一つの MA が必要です。

CFM は MA 内で動作するため，MA を設定することで管理範囲を細かく制御できます。

MA はドメイン名称および MA 名称で識別されます。そのため，同じ MA 内で運用する各装置では，設定時にドメインと MA の名称を合わせておく必要があります。

MA の管理範囲の例を次の図に示します。

図 20-3　MA の管理範囲の例



また，CFM PDU を送受信する VLAN（プライマリ VLAN）を同一 MA 内で合わせておく必要があります。

初期状態では，MA 内で VLAN ID の値がいちばん小さい VLAN がプライマリ VLAN になります。コンフィグレーションコマンド ma vlan-group を使えば，任意の VLAN を明示的にプライマリ VLAN に設定できます。

プライマリ VLAN をデータ転送用の VLAN と同じ VLAN に設定することで，実際の到達性を監視できます。

(3) MEP

MEP はドメインの境界上の管理ポイントで，MA に対して設定します。MEP には MEP ID という MA 内でユニークな ID を設定して各 MEP を識別します。

CFM の機能は MEP で実行されます。CFM は MEP 間（ドメインの境界から境界までの間）で CFM PDU を送受信することで，該当ネットワークの接続性を確認します。

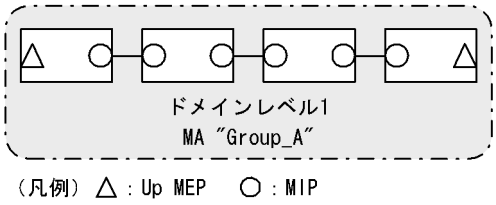
MEP には次の二つの種類があります。

● Up MEP

リレー側に設定する MEP です。Up MEP 自身は CFM PDU を送受信しないで，同一 MA 内の MIP またはポートを介して送受信します。

Up MEP の設定例を次の図に示します。

図 20-4 Up MEP の設定例

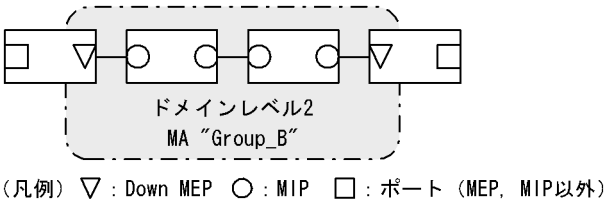


● Down MEP

回線側に設定する MEP です。Down MEP 自身が CFM PDU を送受信します。

Down MEP の設定例を次の図に示します。

図 20-5 Down MEP の設定例



Down MEP，Up MEP からの送信例，および Down MEP，Up MEP での受信例を次の図に示します。

図 20-6　Down MEP，Up MEP からの送信

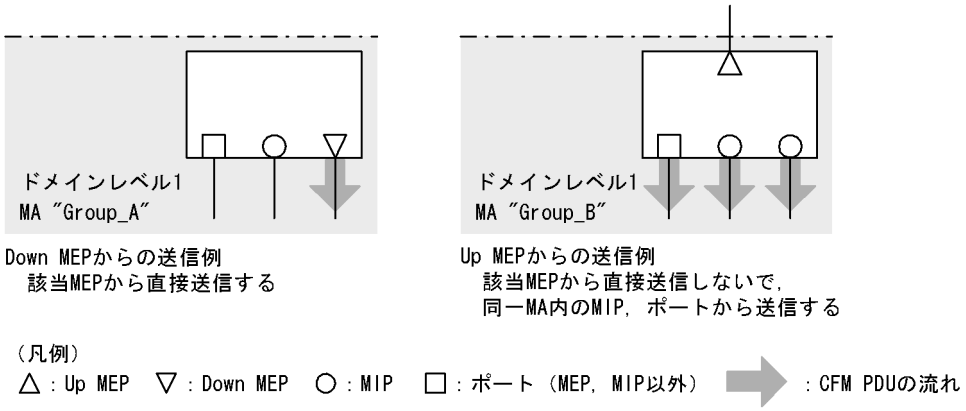
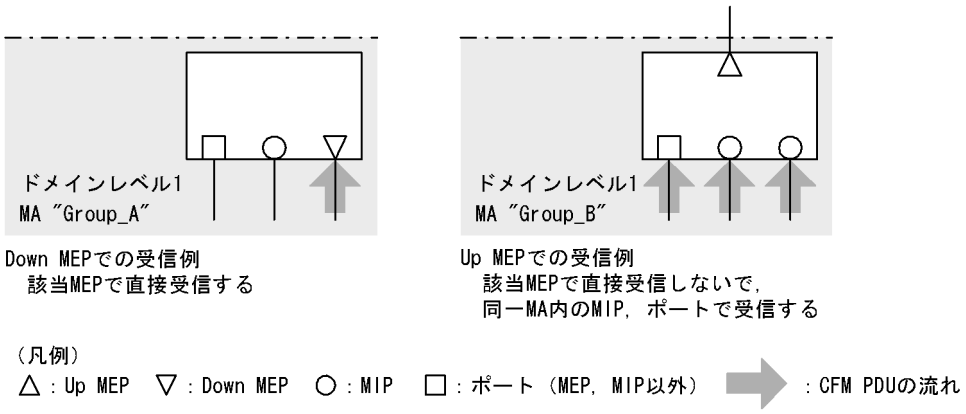
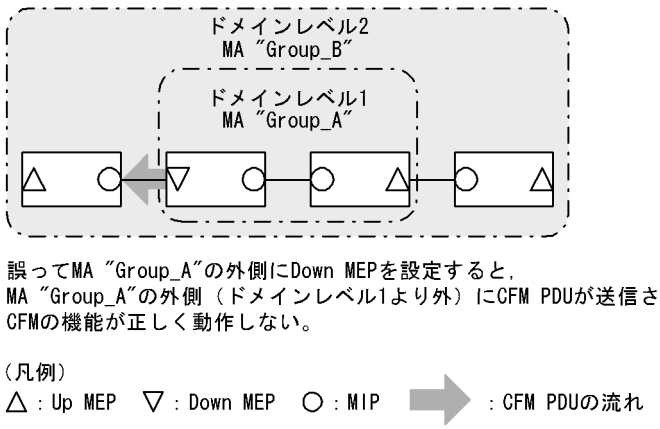


図 20-7　Down MEP，Up MEP での受信



Down MEP および Up MEP は正しい位置に設定してください。例えば，Down MEP は回線側（MA の内側）に設定する必要があります。リレー側（MA の外側）に対して設定した場合，CFM PDU が MA の外側に送信されるため，CFM の機能が正しく動作しません。誤って Down MEP を設定した例を次の図に示します。

図 20-8　誤って Down MEP を設定した例



(4) MIP

MIP はドメインの内部に設定する管理ポイントで，ドメインに対して設定します（同一ドメイン内の全

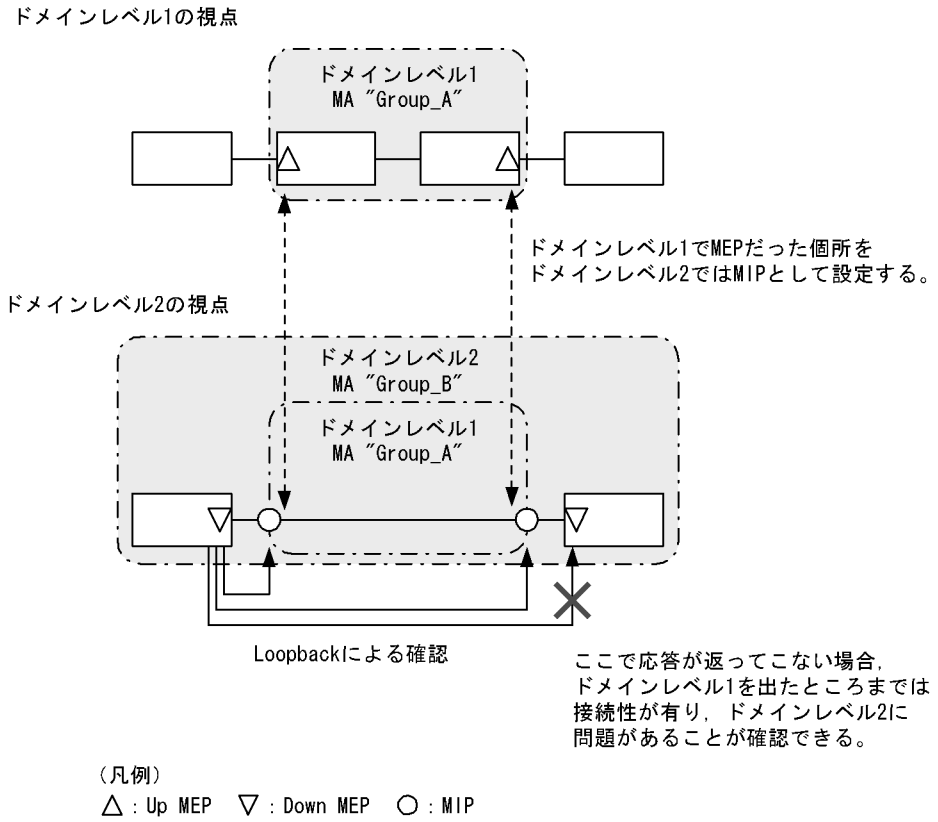
MA で共通)。階層構造の場合，MIP は高いドメインレベルのドメインが低いドメインレベルのドメインと重なる個所に設定します。また，MIP は Loopback および Linktrace に応答するので，ドメイン内の保守管理したい個所に設定します。

(a) ドメインが重なる個所に設定する場合

ドメインが重なる個所に MIP を設定すると，上位ドメインでは，低いドメインを認識しながらも，低いドメインの構成を意識しない状態で管理できます。

ドメインレベル 1 とドメインレベル 2 を使った階層構造の例を次の図に示します。

図 20-9 ドメインレベル 1 とドメインレベル 2 の階層構造の例



ドメインレベル 2 を設計する際，ドメインレベル 1 の MA で MEP に設定しているポートをドメインレベル 2 の MIP として設定します。これによって，ドメインレベル 2 ではドメインレベル 1 の範囲を認識しながらも，運用上は意識しない状態で管理できます。

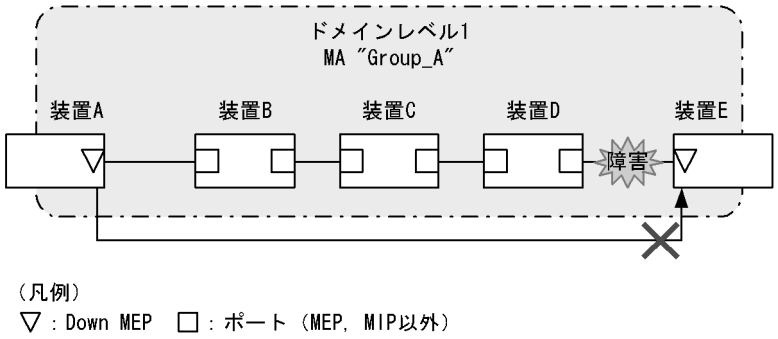
障害発生時は，ドメインレベル 2 の問題か，ドメインレベル 1 のどこかの問題かを切り分けられるため，調査範囲を特定できます。

(b) 保守管理したい個所に設定する場合

ドメイン内で細かく MIP を設定すれば，より細かな保守管理ができるようになります。

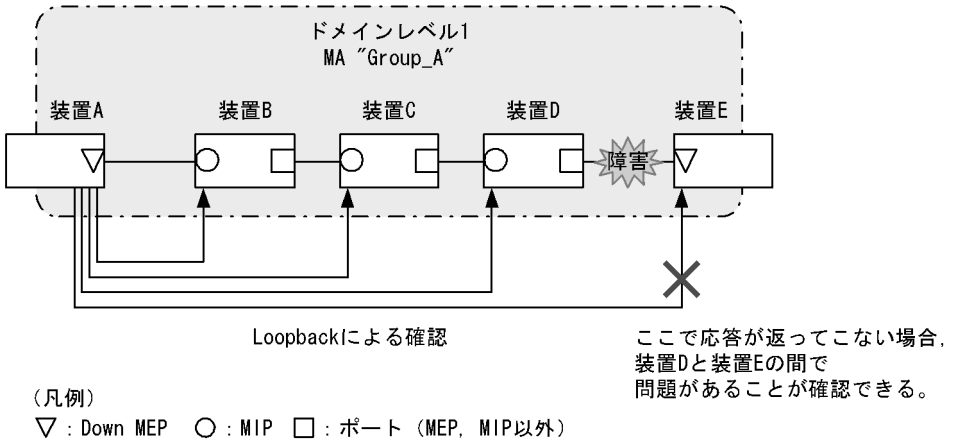
ドメイン内に MIP が設定されていない構成の例を次の図に示します。この例では，ネットワークに障害が発生した場合，装置 A，装置 E の MEP 間で通信できないことは確認できますが，どこで障害が発生したのか特定できません。

図 20-10　ドメイン内に MIP が設定されていない構成の例



ドメイン内に MIP を設定した構成の例を次の図に示します。この例では，ドメイン内に MIP を設定することで，Loopback や Linktrace の応答が各装置から返ってくるため，障害発生個所を特定できるようになります。

図 20-11　ドメイン内に MIP を設定した構成の例



20.1.3　ドメインの設計

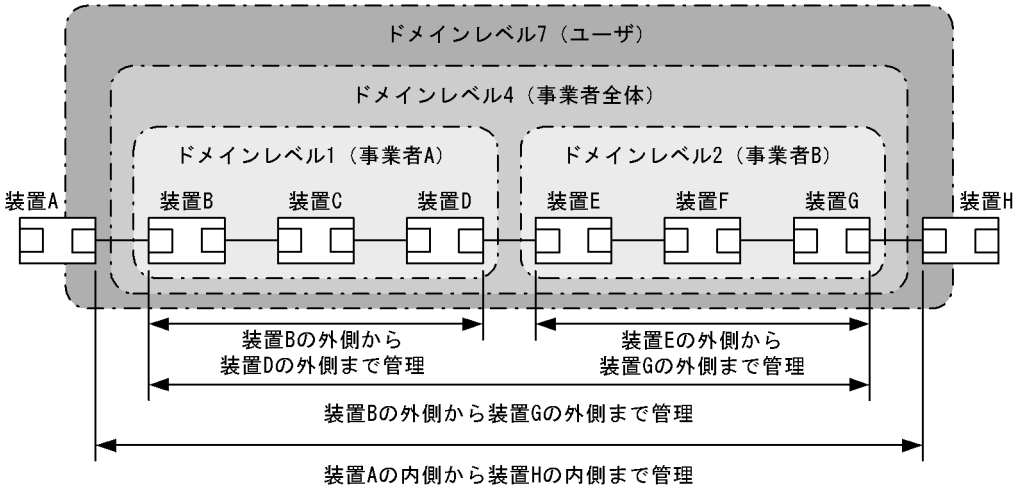
CFM を使用する際には，まずドメインを設計します。ドメインの構成と階層構造を設計し，次に個々のドメインの詳細設計をします。

ドメインの設計には，ドメインレベル，MA，MEP および MIP の設定が必要です。

(1) ドメインの構成と階層構造の設計

ドメインの境界となる MA のポートを MEP に設定し，低いドメインと重なるポートを MIP に設定します。次に示す図の構成例を基に，ドメインの構成および階層構造の設計手順を示します。

図 20-12　構成例



（凡例）□：ポート

事業者 A，事業者 B，事業者全体，ユーザという単位でドメインを設計し，区分に応じたドメインレベルを設定します。また，次の項目を想定しています。

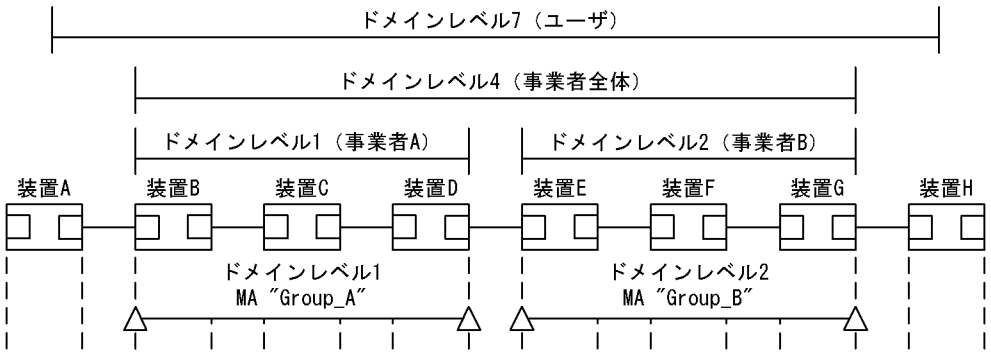
- 事業者 A，事業者 B，事業者全体は，ユーザに提供する回線が利用できることを保障するために，ユーザに提供するポートを含めた接続性を管理
- ユーザは，事業者の提供する回線が使用できるかどうかを監視するために，事業者から提供される回線の接続性を管理

ドメインの設計は，次に示すように低いレベルから順に設定します。

- **ドメインレベル 1，2 の設定**

1. ドメインレベル 1 で MA “ Group_A ” を設定します。
   この例では，一つのドメインを一つの MA で管理していますが，ドメイン内を VLAN グループ単位に分けて詳細に管理したい場合は，管理する単位で MA を設定します。
2. ドメインの境界に当たる装置 B，D で，MA のポートに MEP を設定します。
   事業者はユーザに提供するポートを含めた接続性を管理するため，Up MEP を設定します。
3. ドメインレベル 2 も同様に，MA を設定し，装置 E，G に Up MEP を設定します。

図 20-13　ドメインレベル 1，2 の設定

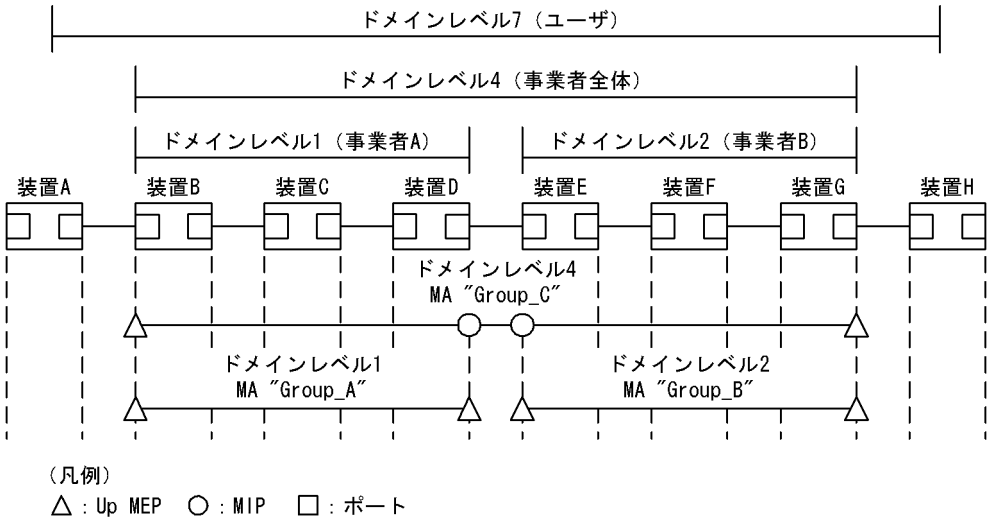


（凡例）
△：Up MEP　□：ポート

• ドメインレベル 4 の設定

1. ドメインレベル 4 で MA “ Group_C ” を設定します。
2. ドメインレベル 4 の境界に当たる装置 B，G で，MA のポートに MEP を設定します。
   事業者はユーザに提供するポートを含めた接続性を管理するため，Up MEP を設定します。
3. ドメインレベル 4 はドメインレベル 1 と 2 を包含しているため，それぞれの中継点である装置 D，E に MIP を設定します。
   低いドメインの MEP を高いドメインで MIP に設定すると，Loopback や Linktrace を使って自分で管理するドメインでの問題か，低いレベルで管理するドメインでの問題かを切り分けられるため，調査範囲を特定しやすくなります。

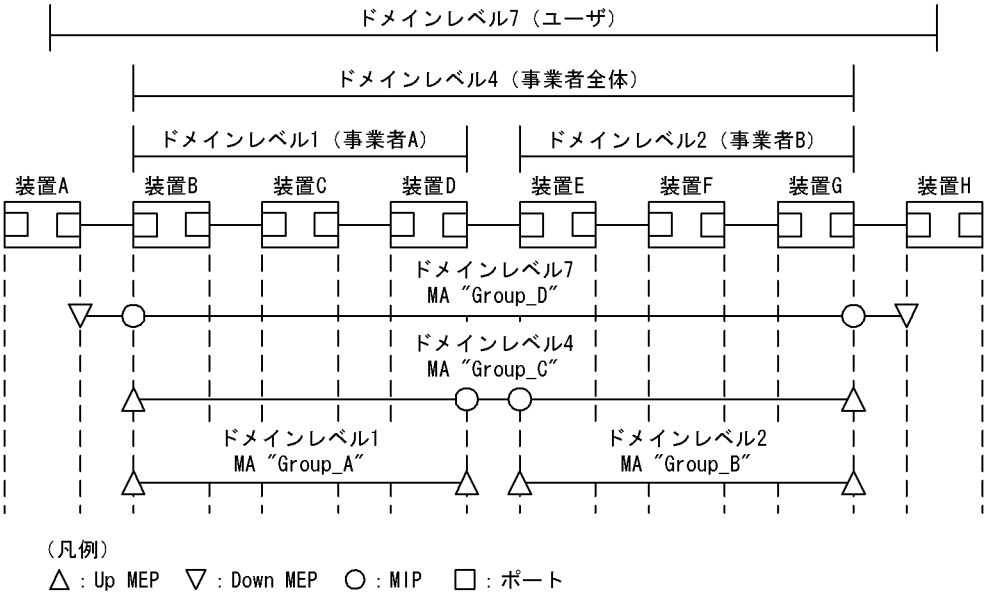
図 20-14　ドメインレベル 4 の設定



• ドメインレベル 7 の設定

1. ドメインレベル 7 で MA “ Group_D ” を設定します。
2. ドメインレベル 7 の境界に当たる A，H で，MA のポートに MEP を設定します。
   ユーザは事業者から提供される回線の接続性を管理するため，Down MEP を設定します。
3. ドメインレベル 7 はドメインレベル 4 を包含しているため，中継点である装置 B，G に MIP を設定します。
   ドメインレベル 1 と 2 は，ドメインレベル 4 の中継点として設定しているため，ドメインレベル 7 では設定する必要はありません。

図 20-15　ドメインレベル 7 の設定



(2) 個々のドメインの詳細設計

個々の詳細設計では，Loopback，Linktrace を適用したい個所に MIP を設定します。

MIP 設定前の構成および MIP 設定後の構成の例を次の図に示します。

図 20-16　MIP 設定前の構成例

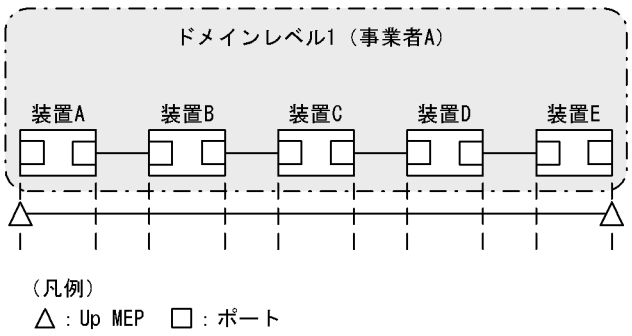
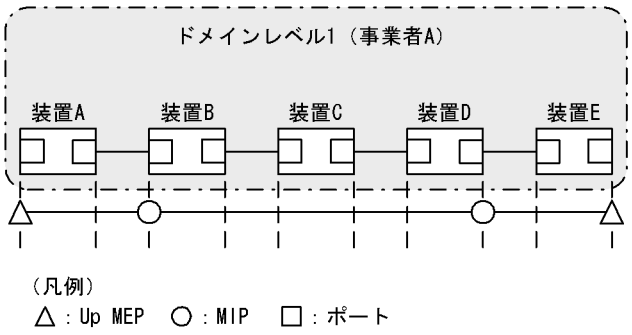


図 20-17　MIP 設定後の構成例



ドメインの内側で Loopback，Linktrace の宛先にしたいポートを MIP に設定します。この例では，装置

B，D に MIP を設定しています。この設定によって装置 B，D の MIP に対し，Loopback，Linktrace を実行できます。また，Linktrace のルート情報として応答を返すようになります。

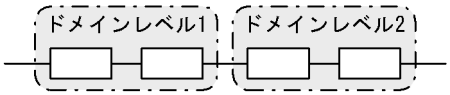
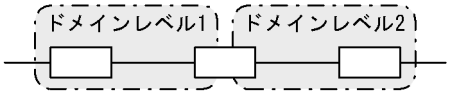
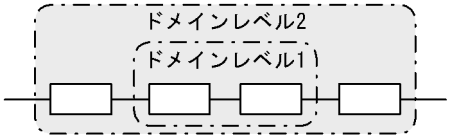
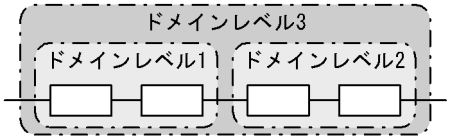
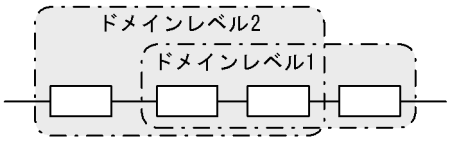
MIP を設定していない装置 C は Loopback，Linktrace の宛先として指定できません。また，Linktrace に応答しないためルート情報に装置 C の情報は含まれません。

(3) ドメインの構成例

ドメインは階層的に設定できますが，階層構造の内側が低いレベル，外側が高いレベルとなるように設定する必要があります。

ドメインの構成例と構成の可否を次の表に示します。

表 20-4 ドメインの構成例と構成の可否

構成状態	構成例	構成の可否
ドメインの隣接		可
ドメインの接触		可
ドメインのネスト		可
ドメインの隣接とネストの組み合わせ		可
ドメインの交差		不可

20.1.4 Continuity Check

Continuity Check（CC）は MEP 間の接続性を常時監視する機能です。MA 内の全 MEP が CCM（Continuity Check Message。CFM PDU の一種）を送受信し合い，MA 内の MEP を学習します。MEP の学習内容は Loopback，Linktrace でも使用します。

CC を動作させている装置で CCM を受信しなくなったり，該当装置の MA 内のポートが通信できない状態になったりした場合に，障害が発生したと見なします。この際，障害検出フラグを立てた CCM を送信し，MA 内の MEP に通知します。

CC で検出する障害を次の表に示します。検出する障害には障害レベルがあります。本装置の初期状態では，障害レベル 2 以上を検出します。

表 20-5　CC で検出する障害

障害レベル	障害内容	初期状態
5	ドメイン，MA が異なる CCM を受信した。	検出する
4	MEP ID または送信間隔が誤っている CCM を受信した。	
3	CCM を受信しなくなった。	
2	該当装置のポートが通信できない状態になった。	
1	障害検出通知の CCM を受信した。 Remote Defect Indication	検出しない

障害回復契機から障害回復監視時間が経過したあと，障害が回復したと見なします。

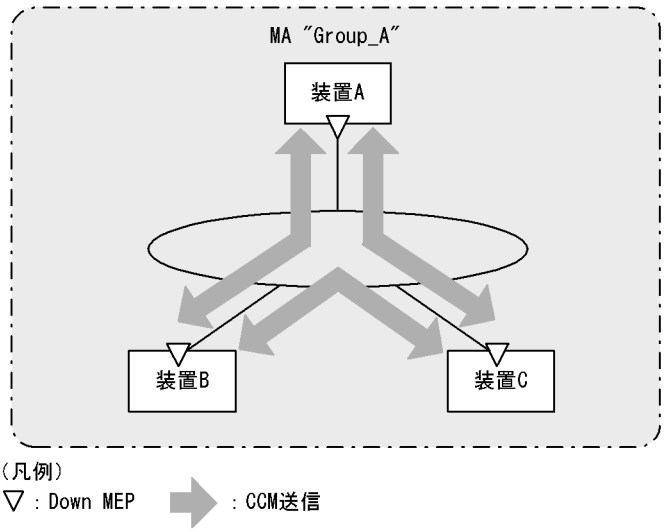
表 20-6　障害回復契機と障害回復監視時間

障害レベル	障害回復契機	障害回復監視時間
5	ドメイン，MA が異なる CCM を受信しなくなった。	受信していた CCM の送信間隔× 3.5
4	MEP ID または送信間隔が誤っている CCM を受信しなくなった。	受信していた CCM の送信間隔× 3.5
3	CCM を再び受信した。	受信した直後から
2	該当装置のポートが通信できる状態になった CCM を受信した。	受信した直後から
1	障害未検出の CCM を受信した。	受信した直後から

次の図の装置 B に着目して CC の動作例を示します。

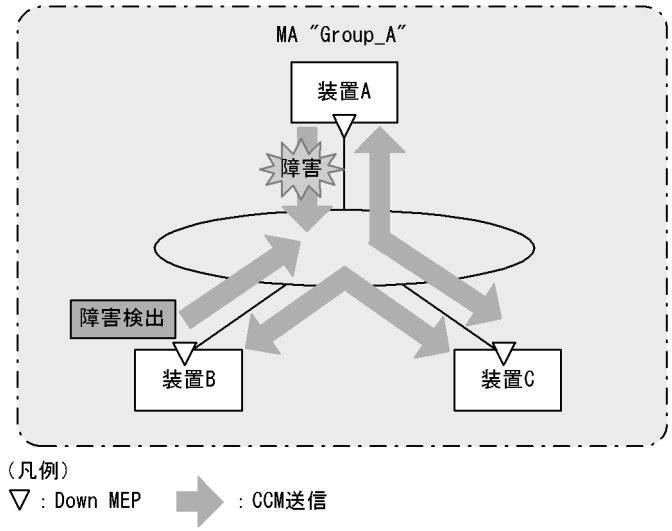
各 MEP はマルチキャストで MA 内に CCM を定期的に送信します。各 MEP の CCM を定期的に受信することで常時接続性を監視します。

図 20-18　CC での常時接続性の監視



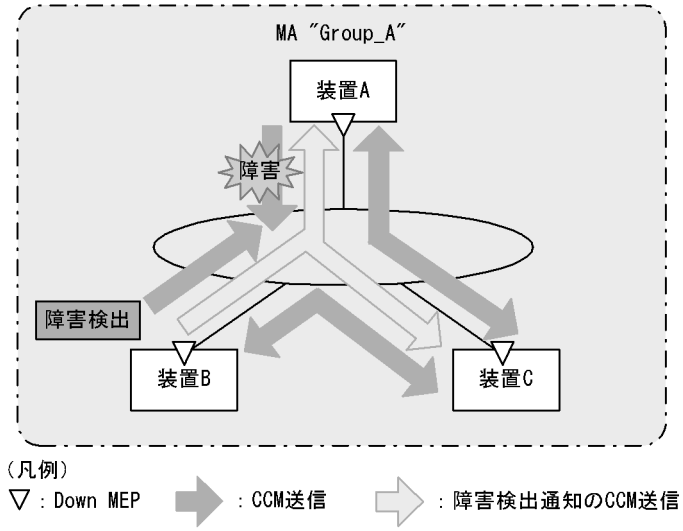
装置 A の CCM が装置の故障またはネットワーク上の障害によって，装置 B に届かなくなると，装置 B は装置 A とのネットワーク上の障害として検出します。

図 20-19　CC で障害を検出



障害を検出した装置 B は，MA 内の全 MEP に対して，障害を検出したことを通知します。

図 20-20　障害を全 MEP に通知



障害検出通知の CCM を受信した各 MEP は，MA 内のどこかで障害が発生したことを認識します。各装置で Loopback，Linktrace を実行することによって，MA 内のどのルートで障害が発生したのかを確認できます。

20.1.5　Loopback

Loopback はレイヤ 2 レベルで動作する，ping 相当の機能です。同一 MA 内の MEP-MEP 間または MEP-MIP 間の接続性を確認します。

CC が MEP-MEP 間の接続性の確認であるのに対し，Loopback では MEP-MIP 間の確認もできるため，MA 内の接続性を詳細に確認できます。

MEP から宛先へループバックメッセージ（CFM PDU の一種）を送信し，宛先から応答が返ってくることを確認することで接続性を確認します。

Loopback には MIP または MEP が直接応答するため，例えば，装置内に複数の MIP を設定した場合，MIP ごとに接続性を確認できます。

MIP および MEP に対する Loopback の実行例を次の図に示します。

図 20-21　MIP に対して Loopback を実行

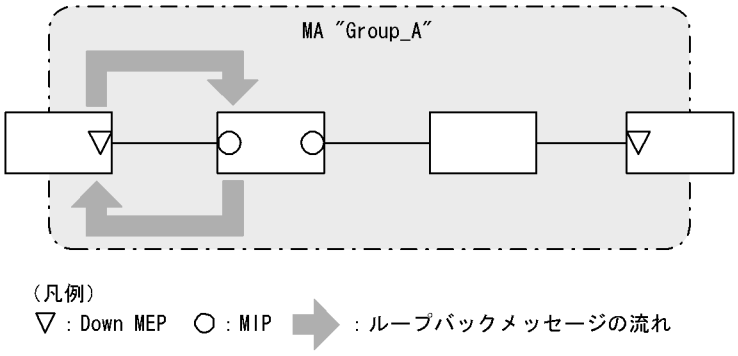
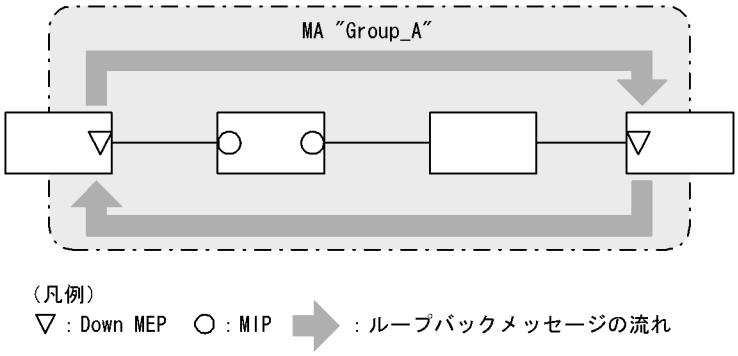


図 20-22　MEP に対して Loopback を実行



Loopback は CC の学習内容を使用するため，事前に CC を動作させておく必要があります。また，宛先に MIP を指定する場合は，事前に MIP のポートの MAC アドレスを調べておく必要があります。

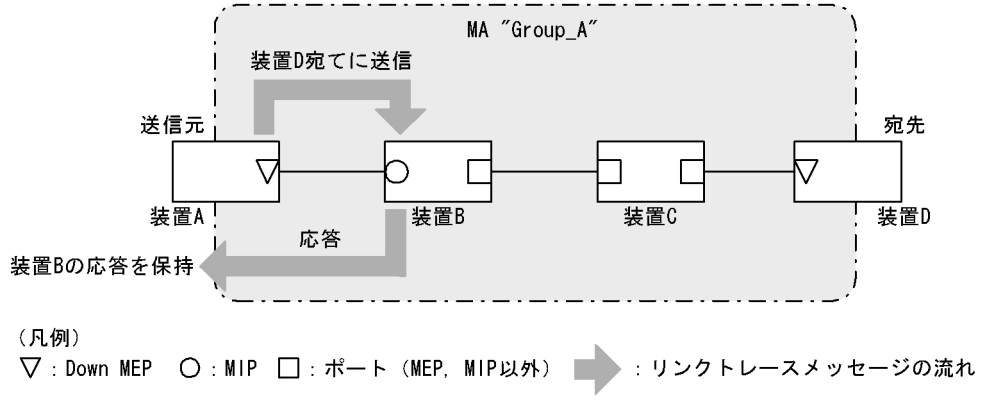
20.1.6　Linktrace

Linktrace はレイヤ 2 レベルで動作する traceroute 相当の機能です。同一 MA 内の MEP-MEP 間または MEP-MIP 間を経由する装置の情報を収集し，ルート情報を出力します。

リンクトレースメッセージ（CFM PDU の一種）を送信し，返ってきた応答をルート情報として収集します。

宛先にリンクトレースメッセージを送信した例を次の図に示します。

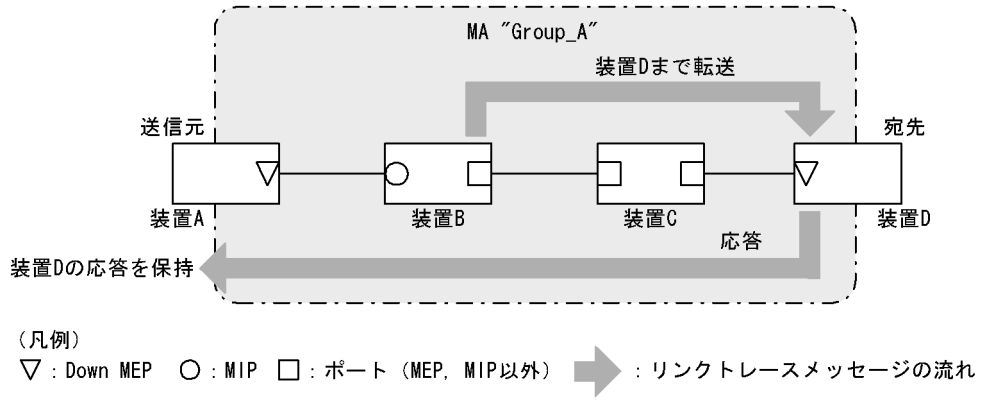
図 20-23　宛先にリンクトレースメッセージを送信



リンクトレースメッセージは宛先まで MIP を介して転送されます。MIP は転送する際に，自装置のどのポートで受信し，どのポートで転送したのかを応答します。送信元装置はルート情報として応答メッセージを保持します。

宛先にリンクトレースメッセージを転送した例を次の図に示します。

図 20-24　宛先にリンクトレースメッセージを転送



応答を返した MIP は宛先までリンクトレースメッセージを転送します。装置 C のように，MEP または MIP が設定されていない装置は応答を返しません（応答を返すには一つ以上の MIP が設定されている必要があります）。

宛先の MEP または MIP までリンクトレースメッセージが到達すると，宛先の MEP または MIP は到達したことと，どのポートで受信したのかを送信元に応答します。

送信元では，保持した応答をルート情報として出力し，宛先までのルートを確認します。

Linktrace は装置単位に応答します。例えば，装置内に設定された MIP が一つでも複数でも，どちらの場合も同じように，受信ポートと転送ポートの情報を応答します。

Linktrace は CC の学習内容を使用するため，事前に CC を動作させておく必要があります。また，宛先に MIP を指定する場合は，事前に MIP のポートの MAC アドレスを調べておく必要があります。

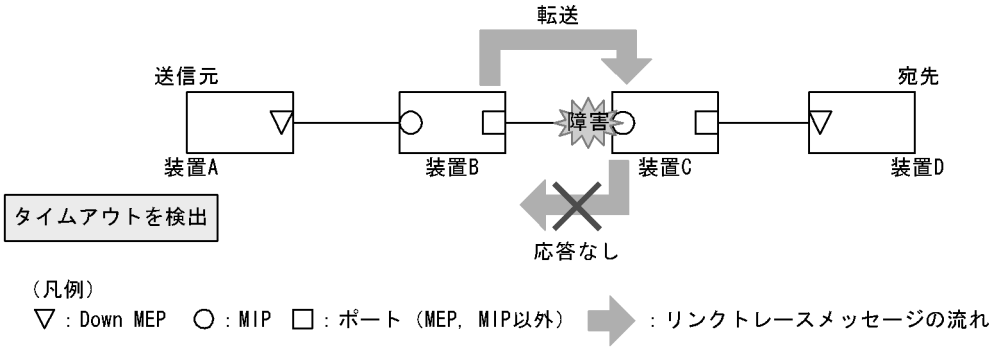
(a) Linktrace による障害の切り分け

Linktrace の実行結果によって，障害が発生した装置やポートなどを絞り込めます。

- **タイムアウトを検出した場合**

Linktrace でタイムアウトを検出した例を次の図に示します。

図 20-25 Linktrace でタイムアウトを検出した例

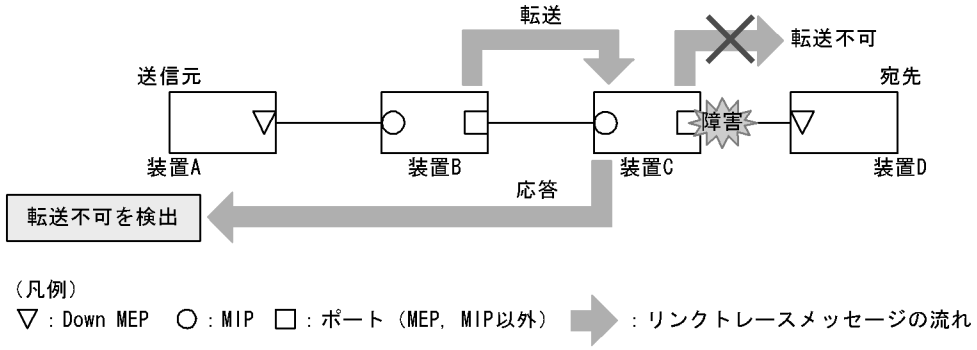


この例では，装置 A が Linktrace でタイムアウトを検出した場合，ネットワーク上の受信側のポートが通信できない状態が考えられます。リンクトレースメッセージが装置 B から装置 C に転送されていますが，装置 C が通信できない状態になっていて，応答を返さないため，タイムアウトになります。

- **転送不可を検出した場合**

Linktrace で通信不可を検出した例を次の図に示します。

図 20-26 Linktrace で通信不可を検出した例



装置 A が Linktrace での転送不可を検出した場合，ネットワーク上の送信側のポートが通信できない状態が考えられます。これは，装置 C が装置 D（宛先）にリンクトレースメッセージを転送できなかった場合，装置 A に送信側ポートが通信できない旨の応答を返すためです。

(b) Linktrace の応答について

リンクトレースメッセージはマルチキャストフレームです。

CFM が動作している装置でリンクトレースメッセージを転送する際には，MIP CCM データベースと MAC アドレステーブルを参照して，どのポートで転送するか決定します。

CFM が動作していない装置ではリンクトレースメッセージをフラッディングします。このため，CFM が動作していない装置がネットワーク上にある場合，宛先のルート以外の装置からも応答が返ります。

20.1.7 共通動作仕様

(1) ブロック状態のポートでの動作

CFM の各機能について，ブロック状態のポートでの動作を次の表に示します。

表 20-7 Up MEP がブロック状態の場合

機能	動作
CC	• CCM を送受信する。送信する CCM のポート状態には Blocked を設定する
Loopback	• 運用コマンド l2ping は実行できない • 自宛のループバックメッセージに応答する
Linktrace	• 運用コマンド l2traceroute は実行できない • リンクトレースメッセージに応答する。応答するリンクトレースメッセージの Egress Port の状態には Blocked を設定する

表 20-8 Down MEP がブロック状態の場合

機能	動作
CC	• CCM を送受信しない
Loopback	• 運用コマンド l2ping は実行できない • 自宛のループバックメッセージに応答しない
Linktrace	• 運用コマンド l2traceroute は実行できない • リンクトレースメッセージに応答しない

表 20-9 MIP がブロック状態の場合

機能	動作
CC	• CCM を透過しない
Loopback	• 回線側から受信した自宛のループバックメッセージに応答しない • リレー側から受信した自宛のループバックメッセージに応答する • ループバックメッセージを透過しない
Linktrace	• 回線側から受信したリンクトレースメッセージに応答しない • リレー側から受信したリンクトレースメッセージに応答する。応答するリンクトレースメッセージの Egress Port の状態には Blocked を設定する • リンクトレースメッセージを透過しない

表 20-10 MEP，MIP 以外のポートがブロック状態の場合

機能	動作
CC	• CCM を透過しない
Loopback	• ループバックメッセージを透過しない
Linktrace	• リンクトレースメッセージを透過しない

(2) VLAN トンネル構成での設定について

VLAN トンネリング網で CFM を使用する場合，VLAN トンネリング網内と VLAN トンネリング網外でドメインを分け，それぞれで管理します。なお，ドメインの設定個所によっては，CFM の機能の使用に一部制限があります。ドメインの設定個所別の機能の使用制限について次の表に示します。

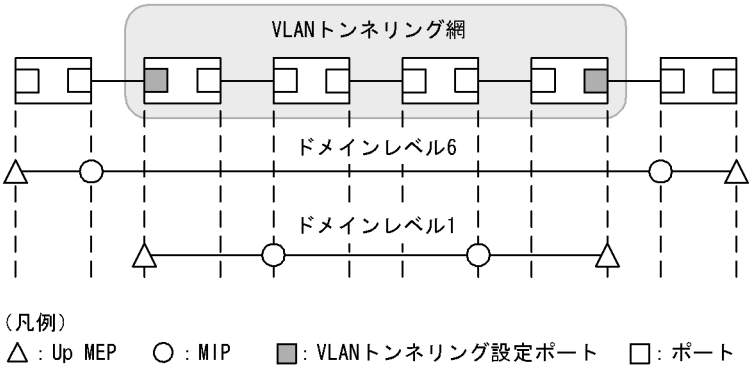
表 20-11 ドメインの設定個所別の機能の使用制限

ドメインの設定個所	機能		
	CC	Loopback	Linktrace
VLAN トンネリング網内と VLAN トンネリング網外	使用可	使用可	• VLAN トンネリング網内では使用可 • VLAN トンネリング網外では VLAN トンネルを越えては使用不可
VLAN トンネリング網内だけ	使用可	使用可	使用可
VLAN トンネリング網外だけ	使用可	使用可	使用可

(a) VLAN トンネリング網内と VLAN トンネリング網外で CFM を使用する場合

VLAN トンネリング網内と VLAN トンネリング網外で CFM を使用する例を次の図に示します。

図 20-27 VLAN トンネリング網内と VLAN トンネリング網外で CFM を使用する例



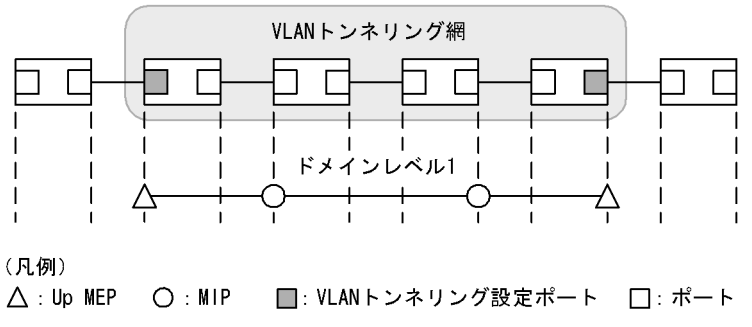
VLAN トンネリング網内のドメインレベル 1 は，VLAN トンネリング網内で任意の個所に管理ポイントを設定できます。VLAN トンネリング網外のドメインレベル 6 は，VLAN トンネリング網外の装置だけに管理ポイントを設定できます。VLAN トンネリング網内にはドメインレベル 6 の管理ポイントは設定できません。VLAN トンネリング網内の管理はドメインレベル 1 でします。

また，VLAN トンネリング網外のドメインレベル 6 では VLAN トンネルを越えては Linktrace を使用できません。

(b) VLAN トンネリング網内だけで CFM を使用する場合

VLAN トンネリング網内だけで CFM を使用する例を次の図に示します。

図 20-28 VLAN トンネリング網内だけで CFM を使用する例



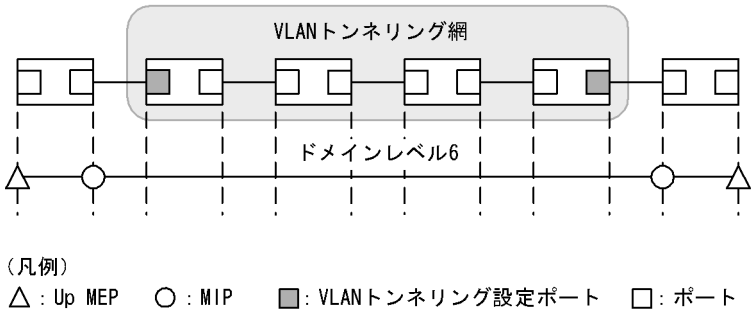
VLAN トンネリング網内のドメインレベル 1 は，VLAN トンネリング網内で任意の個所に管理ポイントを

設定できます。該当ドメインでは CFM の各機能が使用できます。

(c) VLAN トンネリング網外だけで CFM を使用する場合

VLAN トンネリング網外だけで CFM を使用する例を次の図に示します。

図 20-29 VLAN トンネリング網外だけで CFM を使用する例



VLAN トンネリング網外のドメインレベル 6 は，VLAN トンネリング網外の装置だけに管理ポイントを設定できます。VLAN トンネリング網内にはドメインレベル 6 の管理ポイントは設定できません。該当ドメインでは CFM の各機能が使用できます。

20.1.8 CFM で使用するデータベース

CFM で使用するデータベースを次の表に示します。

表 20-12 CFM で使用するデータベース

データベース	内容	内容確認コマンド
MEP CCM データベース	各 MEP が保持しているデータベース。 同一 MA 内の MEP の情報。 CC で常時接続性の監視をする際に使用。 保持する内容は次のとおりです。 • MEP ID • MEP ID に対応する MAC アドレス • 該当 MEP で発生した障害情報	show cfm remote-mep
MIP CCM データベース	装置で保持しているデータベース。 同一ドメイン内の MEP の情報。 リンクトレースメッセージを転送する際，どのポートで転送するかを決定する際に使用。 保持する内容は次のとおりです。 • MEP の MAC アドレス • 該当 MEP の CCM を受信した VLAN とポート	なし
リンクトレースデータベース	Linktrace の実行結果を保持しているデータベース。 保持する内容は次のとおりです。 • Linktrace を実行した MEP と宛先 • TTL • 応答を返した装置の情報 • リンクトレースメッセージを受信したポートの情報 • リンクトレースメッセージを転送したポートの情報	show cfm l2traceroute-db

(1) MEP CCM データベース

MEP CCM データベースは，同一 MA 内にどのような MEP があるかを保持しています。また，該当する MEP で発生した障害情報も保持しています。

Loopback，Linktrace では宛先を MEP ID で指定できますが，MEP CCM データベースに登録されていない MEP ID は指定できません。MEP ID がデータベース内に登録されているかどうかは運用コマンド show cfm remote-mep で確認できます。

本データベースのエントリは CC 実行時に MEP が CCM を受信したときに作成します。

(2) MIP CCM データベース

MIP CCM データベースは，リンクトレースメッセージを転送する際にどのポートから転送すればよいかを決定する際に使用します。

転送時，MIP CCM データベースに宛先 MEP の MAC アドレスが登録されていない場合は，MAC アドレステーブルを参照して転送するポートを決定します。

MAC アドレステーブルにもない場合はリンクトレースメッセージは転送しないで，転送できなかった旨の応答を転送元に返します。

本データベースのエントリは CC 実行時に MIP が CCM を転送したときに作成します。

(3) リンクトレースデータベース

リンクトレースデータベースは，Linktrace の実行結果を保持しています。

運用コマンド show cfm l2traceroute-db で，過去に実行した Linktrace の結果を参照できます。

(a) 保持できるルート数について

装置全体で 1024 装置分の応答を保持します。

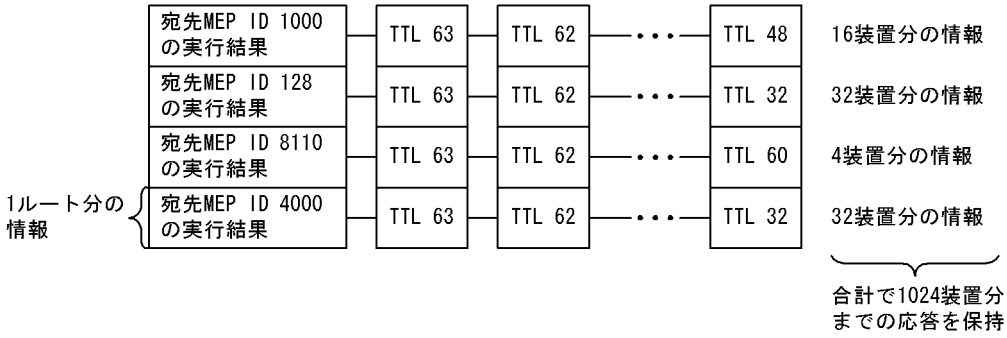
1 ルート当たり何装置分の応答を保持するかで何ルート分保持できるかが決ります。1 ルート当たり 256 装置分の応答を保持した場合は 4 ルート，1 ルート当たり 16 装置分の応答を保持している場合は 64 ルート保持できます。

応答が 1024 装置分を超えた場合，古いルートの情報が消去され，新しいルートの情報を保持します。

リンクトレースデータベースに登録されている宛先に対して Linktrace を実行した場合，リンクトレースデータベース上から該当宛先までのルート情報を削除したあとに新しい Linktrace の応答を保持します。

リンクトレースデータベースを次の図に示します。

図 20-30 リンクトレースデータベース



本データベースのエントリは Linktrace 実行時に MEP が応答を受信したときに作成します。

20.1.9 CFM 使用時の注意事項

(1) CFM を動作させない装置について

CFM を適用する際，ドメイン内の全装置で CFM を動作させる必要はありませんが，CFM を動作させない装置では CFM PDU を透過させる必要があります。

本装置を除き，CFM を動作させない装置は，次の表に示すフレームを透過するように設定してください。

表 20-13 透過させるフレーム

フレーム種別	宛先 MAC アドレス
マルチキャスト	0180.c200.0030 ～ 0180.c200.003f

本装置は，CFM が動作していない場合はすべての CFM PDU を透過します。

(2) 他機能との共存について

次に示す機能とは同時に使用できません。

- LLDP
- OADP

次に示すポートでは同時に使用できません。

- レイヤ 2 認証設定ポート

(3) CFM PDU のバースト受信について

CC で常時監視するリモート MEP 数が 48 以上あると，リモート MEP からの CFM PDU 送信タイミングが偶然一致した場合に，本装置で CFM PDU をバースト受信することがあります。その場合，本装置で CFM PDU を廃棄することがあり，障害を誤検出するおそれがあります。

本現象が頻発する場合は，各装置での CFM PDU の送信タイミングが重ならないように調整してください。

(4) 同一ドメインで同一プライマリ VLAN を設定している MA での MEP 設定について

同一ドメインで同一プライマリ VLAN を設定している MA（同一 MA も含む）で，同一ポートに対して 2 個以上の MEP を設定できません。設定した場合は，該当する MEP で CFM が正常に動作しません。

(5) Linktrace でのルート情報の収集について

Linktrace ではリンクトレースメッセージの転送先ポートは，MIP CCM データベースまたは MAC アドレステーブルを参照して決定します。そのため，リンクアップ時（リンクダウン後の再アップ含む）やスパニングツリーなどによる経路変更後は，CC で CCM を送受信するまで転送先ポートが決定できないため，正しいルート情報の収集ができません。

(6) Up MEP および MIP で CFM が動作しないタイミング

次のイベント発生後に，一度もリンクアップしていない Up MEP および MIP のポートでは CFM の各機能が動作しません。一度リンクアップさせることで動作します。

- 装置起動（装置再起動も含む）
- コンフィグレーションファイルのランニングコンフィグレーションへの反映

- 運用コマンド restart vlan の実行
- 運用コマンド restart cfm の実行

（7） ブロック状態のポートで MIP が Loopback，Linktrace に応答しない場合について

ブロック状態のポートに MIP を設定し，該当ポートで次に示す運用をした場合，MIP は Loopback，Linktrace に応答しないことがあります。

- スパニングツリー（PVST+，シングル）でループガード機能を運用
- スパニングツリー（MSTP）の運用時に，アクセス VLAN またはネイティブ VLAN をプライマリ VLAN として設定

（8） 冗長構成での CC の動作について

スパニングツリーなどの冗長構成を組んだネットワーク上で CC を運用している場合，通信経路の切り替えが発生したときに，まれに自装置の MEP が送信した CCM を受信して ErrorCCM を検出することがあります。本障害は通信経路が安定すると回復します。

20.2 コンフィグレーション

20.2.1 コンフィグレーションコマンド一覧

CFM 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。

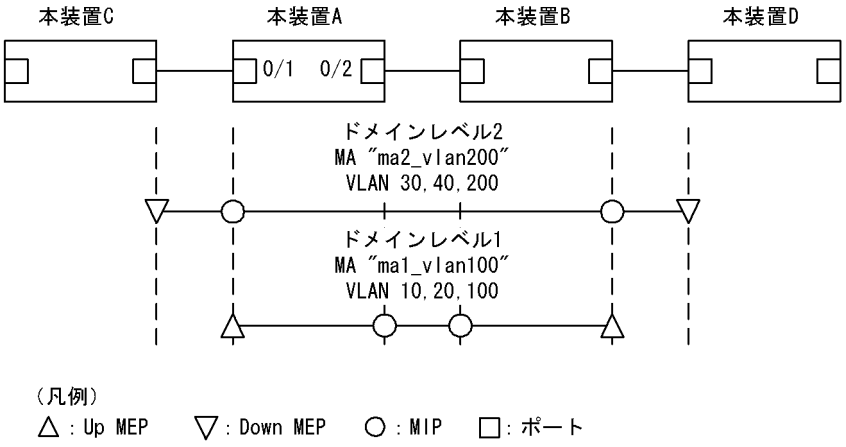
表 20-14 コンフィグレーションコマンド一覧

コマンド名	説明
domain name	該当ドメインで使用する名称を設定します。
ethernet cfm cc alarm-priority	CC で検知する障害レベルを設定します。
ethernet cfm cc alarm-reset-time	CC で障害を再検知と見なすまでの時間を設定します。
ethernet cfm cc alarm-start-time	CC で障害を検知してからトラップを通知するまでの時間を設定します。
ethernet cfm cc enable	ドメインで CC を使用する MA を設定します。
ethernet cfm cc interval	CCM の送信間隔を設定します。
ethernet cfm domain	ドメインを設定します。
ethernet cfm enable (global)	CFM を開始します。
ethernet cfm enable (interface)	no ethernet cfm enable 設定時に CFM を停止します。
ethernet cfm mep	CFM で使用する MEP を設定します。
ethernet cfm mip	CFM で使用する MIP を設定します。
ma name	該当ドメインで使用する MA の名称を設定します。
ma vlan-group	該当ドメインで使用する MA に所属する VLAN を設定します。

20.2.2 CFM の設定（複数ドメイン）

複数ドメインを設定する手順を説明します。ここでは，次の図に示す本装置 A の設定例を示します。

図 20-31 CFM の設定例（複数ドメイン）



(1) 複数ドメインおよびドメインごとの MA の設定

[設定のポイント]

複数のドメインがある場合，低いドメインレベルのドメインから設定します。MA の設定はドメイン

レベルと MA 識別番号，ドメイン名称，および MA 名称を対向装置と一致させる必要があります。設定が異なる場合，本装置と対向装置は同一 MA と判断されません。
MA のプライマリ VLAN には，本装置の MEP から CFM PDU を送信する VLAN を設定します。
primary-vlan パラメータが設定されていない場合は，vlan-group パラメータで設定された VLAN の中から，最も小さな VLAN ID を持つ VLAN がプライマリ VLAN になります。

[コマンドによる設定]

1. **(config)# ethernet cfm domain level 1 direction-up**
   (config-ether-cfm)# domain name str operator_1
   ドメインレベル 1 と MEP の初期状態を Up MEP にすることを設定します。コンフィグレーションイーサネット CFM モードに移行し，ドメイン名称を設定します。

2. **(config-ether-cfm)# ma 1 name str ma1_vlan100**
   (config-ether-cfm)# ma 1 vlan-group 10,20,100 primary-vlan 100
   (config-ether-cfm)# exit
   MA1 で MA 名称，MA に所属する VLAN，プライマリ VLAN を設定します。

3. **(config)# ethernet cfm domain level 2**
   (config-ether-cfm)# domain name str operator_2
   (config-ether-cfm)# ma 2 name str ma2_vlan200
   (config-ether-cfm)# ma 2 vlan-group 30,40,200 primary-vlan 200
   (config-ether-cfm)# exit
   ドメインレベル 2 と MEP の初期状態を Down MEP にすることを設定します。
   MA2 で MA 名称，MA に所属する VLAN，プライマリ VLAN を設定します。

(2) MEP および MIP の設定

[設定のポイント]

MEP および MIP の設定数は，収容条件数以内に収まるように設定してください。
設定した MEP および MIP の運用を開始するには，装置の CFM を有効にする設定が必要になります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# ethernet cfm mep level 1 ma 1 mep-id 101
   (config-if)# ethernet cfm mip level 2
   (config-if)# exit
   (config)# interface gigabitethernet 0/2
   (config-if)# ethernet cfm mip level 1
   (config-if)# exit
   ポート 0/1 に，ドメインレベル 1，MA1 に所属する MEP を設定します。また，ドメインレベル 2 の MIP を設定します。ポート 0/2 にドメインレベル 1 の MIP を設定します。

2. **(config)# ethernet cfm enable**
   本装置の CFM の運用を開始します。

(3) ポートの CFM の停止

[設定のポイント]

一時的にポートの CFM を停止したい場合に設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# no ethernet cfm enable
   (config-if)# exit
   ポート 0/1 の CFM を停止します。

(4) CC の設定

[設定のポイント]

ethernet cfm cc enable コマンドの設定直後から，CC が動作します。

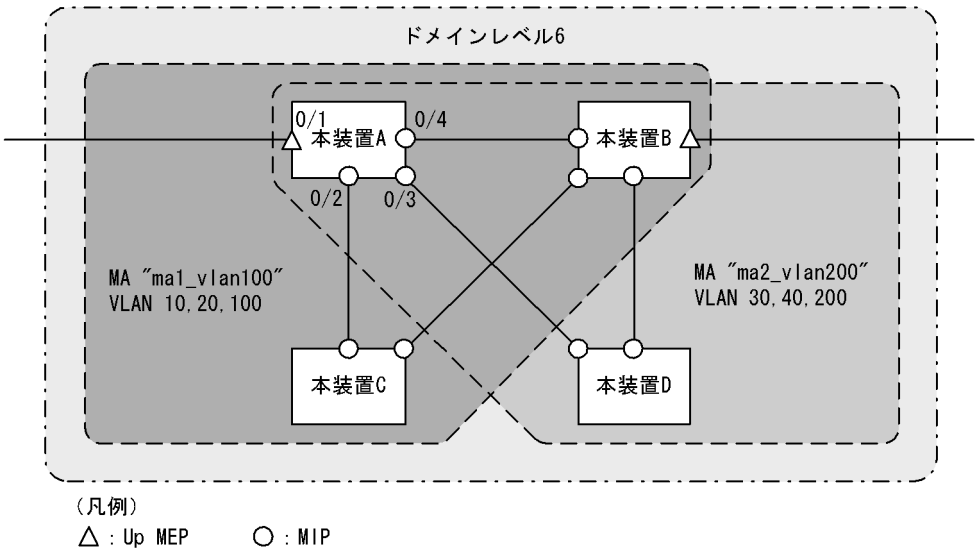
[コマンドによる設定]

1. **(config)# ethernet cfm cc level 1 ma 1 interval 10s**
   (config)# ethernet cfm cc level 1 ma 1 enable
   ドメインレベル 1，MA1 で，CCM の送信間隔を 10 秒に設定したあとに CC の動作を開始します。

20.2.3 CFM の設定（同一ドメイン，複数 MA）

同一ドメインで複数の MA を設定する手順を説明します。ここでは，次の図に示す本装置 A の設定例を示します。

図 20-32 CFM の設定例（同一ドメイン，複数 MA）



(1) 同一ドメインでの複数 MA の設定

[設定のポイント]

同一ドメインで複数の MA を設定する場合は，MA 識別番号および MA 名称が重複しないように設定します。ドメインおよび MA の基本的な設定のポイントは，「20.2.2 CFM の設定（複数ドメイン）」

を参照してください。

[コマンドによる設定]

1. **(config)# ethernet cfm domain level 6 direction-up**
   (config-ether-cfm)# domain name str customer_6
   ドメインレベルと MEP の初期状態を Up MEP にすることを設定します。コンフィグレーションイーサネット CFM モードに移行し，ドメイン名称を設定します。

2. **(config-ether-cfm)# ma 1 name str ma1_vlan100**
   (config-ether-cfm)# ma 1 vlan-group 10,20,100 primary-vlan 100
   (config-ether-cfm)# ma 2 name str ma2_vlan200
   (config-ether-cfm)# ma 2 vlan-group 30,40,200 primary-vlan 200
   (config-ether-cfm)# exit
   MA 識別番号と MA 名称，MA に所属する VLAN，プライマリ VLAN を設定します。

(2) MEP および MIP の設定

[設定のポイント]

MEP は MA ごとに設定する必要があります。MIP は複数の MA で共通で，ポート単位に一つ設定します。MEP および MIP の基本的な設定のポイントは，「20.2.2　CFM の設定（複数ドメイン）」を参照してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# ethernet cfm mep level 6 ma 1 mep-id 101
   (config-if)# ethernet cfm mep level 6 ma 2 mep-id 201
   (config-if)# exit
   (config)# interface range gigabitethernet 0/2-4
   (config-if-range)# ethernet cfm mip level 6
   (config-if-range)# exit
   ポート 0/1 に，ドメインレベル 6，MA1 に所属する MEP を設定します。また，MA2 に所属する MEP を設定します。ポート 0/2 ～ 0/4 にドメインレベル 6 の MIP を設定します。

2. **(config)# ethernet cfm enable**
   本装置の CFM の運用を開始します。

20.3 オペレーション

20.3.1 運用コマンド一覧

CFM の運用コマンド一覧を次の表に示します。

表 20-15 運用コマンド一覧

コマンド名	説明
l2ping	CFM の Loopback 機能を実行します。指定 MP 間の接続を確認します。
l2traceroute	CFM の Linktrace 機能を実行します。指定 MP 間のルートを確認します。
show cfm	CFM のドメイン情報を表示します。
show cfm remote-mep	CFM のリモート MEP の情報を表示します。
show cfm fault	CFM の障害情報を表示します。
show cfm l2traceroute-db	l2traceroute コマンドで取得したルート情報を表示します。
show cfm statistics	CFM の統計情報を表示します。
clear cfm remote-mep	CFM のリモート MEP 情報をクリアします。
clear cfm fault	CFM の障害情報をクリアします。
clear cfm l2traceroute-db	l2traceroute コマンドで取得したルート情報をクリアします。
clear cfm statistics	CFM の統計情報をクリアします。
restart cfm	CFM プログラムを再起動します。
dump protocols cfm	CFM のダンプ情報をファイルへ出力します。

20.3.2 MP 間の接続確認

l2ping コマンドで，指定した MP 間の疎通を確認して，結果を表示します。コマンドには確認回数および応答待ち時間を指定できます。指定しない場合，確認回数は 5 回，応答待ち時間は 5 秒です。疎通確認の応答受信または応答待ち時間経過を契機に，次の確認を繰り返します。

図 20-33 l2ping コマンドの実行結果

```
>l2ping remote-mep 1010 domain-level 7 ma 1000 mep 1020 count 3 timeout 1
L2ping to MP:1010(0012.e220.00a3) on Level:7  MA:1000  MEP:1020  VLAN:20
Time:2009/03/14 19:10:24
1: L2ping Reply from 0012.e220.00a3  64bytes  Time=  751 ms
2: L2ping Reply from 0012.e220.00a3  64bytes  Time=  752 ms
3: L2ping Reply from 0012.e220.00a3  64bytes  Time=  744 ms

--- L2ping Statistics ---
Tx L2ping Request :    3  Rx L2ping Reply :    3  Lost Frame  :   0%
Round-trip Min/Avg/Max : 744/749/752 ms

>
```

20.3.3 MP 間のルート確認

l2traceroute コマンドで，指定した MP 間のルート情報を収集し，結果を表示します。コマンドには応答待ち時間と TTL 値を指定できます。指定しない場合，応答待ち時間は 5 秒，TTL 値は 64 です。

宛先に指定した MP から応答を受信したことを「Hit」で確認できます。

図 20-34 l2traceroute コマンドの実行結果

```
>l2traceroute remote-mep 2010 domain-level 7 ma 1000 mep 2020 timeout 10 ttl 64
Date 2009/03/15 14:05:30 UTC
L2traceroute to MP:0012.e220.00a3 on Level:7  MA:1000  MEP:1020  VLAN:1000
Time:2009/03/15 14:05:30
63  0012.e220.00c0  Forwarded
62  0012.e210.000d  Forwarded
61  0012.e242.00a3  NotForwarded  Hit
```

20.3.4 ルート上の MP の状態確認

show cfm l2traceroute-db detail コマンドで，宛先の MP までのルートとルート上の MP の詳細情報を確認できます。「NotForwarded」が表示された場合，Ingress Port および Egress Port の「Action」で，リンクトレースメッセージが中継されなかった理由を確認できます。

図 20-35 show cfm l2traceroute-db detail コマンドの実行結果

```
> show cfm l2traceroute-db remote-mac 0012.e220.1040 detail
Date 2009/03/16 10:21:42 UTC
L2traceroute to MP:2010(0012.e220.1040) on Level:7  MA:2000  MEP:2020  VLAN:20
Time:2009/03/16 10:21:42
63   0012.e220.10a9  Forwarded
  Last Egress : 0012.f110.2400  Next Egress : 0012.e220.10a0
  Relay Action: MacAdrTbl
  Chassis ID    Type: MAC       Info: 0012.e228.10a0
  Ingress Port  MP Address: 0012.e220.10a9  Action: OK
  Egress Port   MP Address: 0012.e220.10aa  Action: OK
62   0012.e228.aa3b  NotForwarded
  Last Egress : 0012.e220.10a0  Next Egress : 0012.e228.aa30
  Relay Action: MacAdrTbl
  Chassis ID    Type: MAC       Info: 0012.e228.aa30
  Ingress Port  MP Address: 0012.e228.aa2c  Action: -
  Egress Port   MP Address: 0012.e228.aa3b  Action: Down
>
```

20.3.5 CFM の状態の確認

show cfm コマンドで，CFM の設定状態と障害検知状態を表示します。CC で障害を検知した場合，検知した障害の中で，最も障害レベルの高い障害種別を「Status」で確認できます。

図 20-36 show cfm コマンドの実行結果

```
>show cfm
Date 2009/03/15 18:32:10 UTC
Domain Level 3 Name(str): ProviderDomain_3
  MA 300   Name(str) : Tokyo_to_Osaka
    Primary VLAN:300   VLAN:10-20,300
    CC:Enable   Interval:1min
    Alarm Priority:3  Start Time:2500ms  Reset Time:10000ms
    MEP Information
      ID:8012  UpMEP    CH12(Up)    Enable   MAC:0012.e200.00b2  Status:Timeout
  MA 400   Name(str) : Tokyo_to_Nagoya
    Primary VLAN:400   VLAN:30-40,400
    CC:Enable   Interval:1min
    Alarm Priority:3  Start Time:2500ms  Reset Time:10000ms
    MEP Information
      ID:8014  DownMEP  0/21(Up)    Disable  MAC:0012.e220.0040  Status:-
  MIP Information
      0/12(Up)    Enable   MAC:0012.e200.0012
      0/22(Down)  Disable  MAC:-
Domain Level 4 Name(str): ProviderDomain_4
  MIP Information
      CH12(Up)    Enable   MAC:0012.e220.00b2
>
```

20.3.6 障害の詳細情報の確認

show cfm fault detail コマンドで，障害種別ごとに，障害検知状態と障害検知のきっかけとなった CCM 情報を表示します。CCM を送信したリモート MEP は「RMEP」,「MAC」および「VLAN」で確認できます。

図 20-37 show cfm fault detail コマンドの実行結果

```
>show cfm fault detail
Date 2009/03/21 12:23:41 UTC
MD:7  MA:1000  MEP:1000  Fault
  OtherCCM : -  RMEP:1020 MAC:0012.e220.1e22 VLAN:1000 Time:2009/03/20 11:22:17
  ErrorCCM : -
  Timeout  : -
  PortState: -
  RDI      : On RMEP:1011 MAC:0012.e220.11a2 VLAN:1000 Time:2009/03/21 11:42:10
>
```

show cfm fault detail コマンドで表示されるリモート MEP 情報は障害検知のきっかけとなった情報であり，実際には複数のリモート MEP で障害が発生しているおそれがあります。

現在どのリモート MEP で障害が発生しているかは，show cfm remote-mep コマンドで表示されるリモート MEP 情報の「ID」および「Status」で確認できます。

図 20-38 show cfm remote-mep コマンドの実行結果

```
>show cfm remote-mep
Date 2009/03/21 12:25:30 UTC
Total RMEP Counts:      5
Domain Level 7 Name(str): ProviderDomain_7
  MA 1000  Name(str) : Tokyo_to_Osaka
    MEP ID:1000  0/20(Up)    Enable   Status:RDI
      RMEP Information  Counts:  3
      ID:1011  Status:-           MAC:0012.e200.005a  Time:2009/03/21 12:25:29
      ID:1020  Status:RDI         MAC:0012.e220.1e22  Time:2009/03/21 12:25:29
      ID:1030  Status:RDI         MAC:0012.e220.1e09  Time:2009/03/21 12:25:29
  MA 2000  Name(str) : Tokyo_to_Nagoya
    MEP ID:8012  CH1 (Up)    Enable   Status:-
      RMEP Information  Counts:  2
      ID:8003  Status:-           MAC:0012.e20a.1241  Time:2009/03/21 12:25:28
      ID:8004  Status:-           MAC:0012.e20d.12a1  Time:2009/03/21 12:25:29
>
```

21 SNMP を使用したネットワーク管理

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

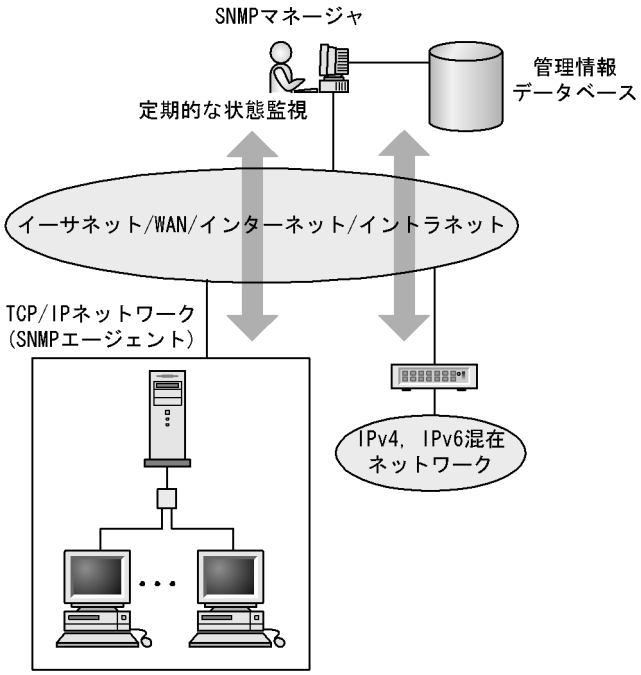
21.1 解説

21.1.1 SNMP 概説

(1) ネットワーク管理

ネットワークシステムの稼働環境や性能を維持するためには，高度なネットワーク管理が必要です。SNMP（simple network management protocol）は業界標準のネットワーク管理プロトコルです。SNMP をサポートしているネットワーク機器で構成されたマルチベンダーネットワークを管理できます。管理情報を収集して管理するサーバを SNMP **マネージャ**，管理される側のネットワーク機器を SNMP **エージェント**といいます。ネットワーク管理の概要を次の図に示します。

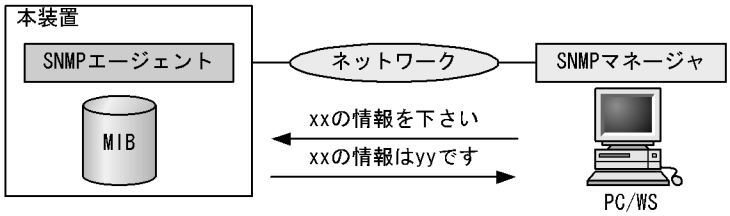
図 21-1 ネットワーク管理の概要



(2) SNMP エージェント機能

本装置の SNMP エージェントは，ネットワーク上の装置内部に組み込まれたプログラムです。装置内の情報を SNMP マネージャに提供する機能があります。装置内にある各種情報を MIB（Management Information Base）と呼びます。SNMP マネージャは，装置の情報を取り出して編集・加工し，ネットワーク管理を行うための各種情報をネットワーク管理者に提供するソフトウェアです。MIB 取得の例を次の図に示します。

図 21-2 MIB 取得の例

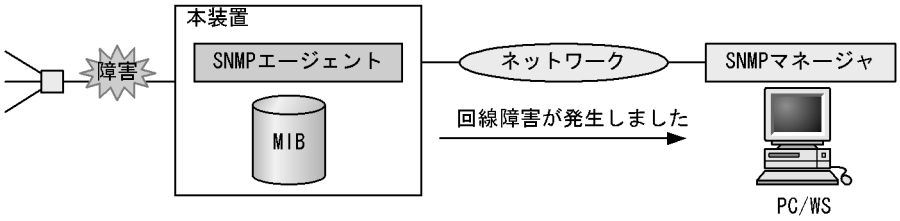


本装置の運用コマンドには MIB 情報を表示するための SNMP コマンドがあります。このコマンドは，自装置およびリモート装置の SNMP エージェントの MIB を表示します。

本装置では，SNMPv1（RFC1157），SNMPv2C（RFC1901），および SNMPv3（RFC3410）をサポートしています。SNMP マネージャを使用してネットワーク管理を行う場合は，SNMPv1，SNMPv2C，または SNMPv3 プロトコルで使用してください。なお，SNMPv1，SNMPv2C，SNMPv3 をそれぞれ同時に使用することもできます。

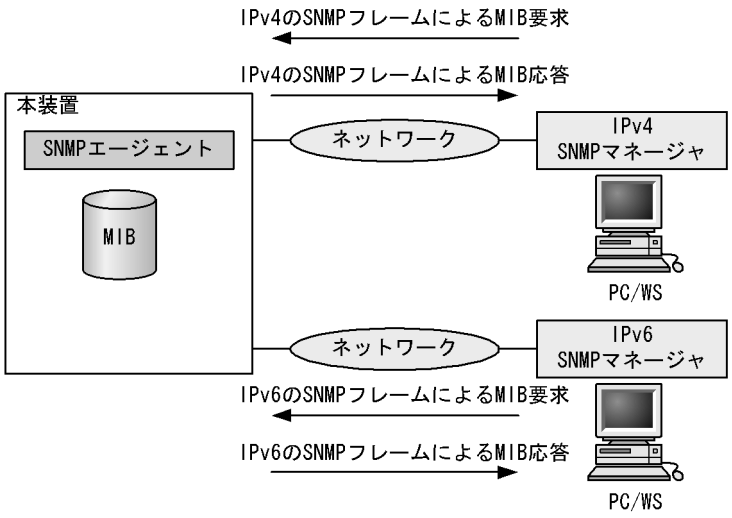
また，SNMP エージェントは**トラップ**（Trap）と呼ばれるイベント通知（主に障害発生の情報など）機能があります。SNMP マネージャは，トラップを受信することで定期的に装置の状態変化を監視しなくても変化を知ることができます。ただし，トラップは UDP を使用しているため，装置から SNMP マネージャに対するトラップの到達確認ができません。そのため，ネットワークの輻輳などによって，トラップがマネージャに到達しない場合があります。トラップの例を次の図に示します。

図 21-3 トラップの例



本装置の SNMP プロトコルは IPv6 に対応しています。コンフィグレーションに設定した SNMP マネージャの IP アドレスによって，IPv4 または IPv6 アドレスが設定されている SNMP マネージャからの MIB 要求や，SNMP マネージャへのトラップ送信ができます。IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例を次の図に示します。

図 21-4 IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例



(3) SNMPv3

SNMPv3 は SNMPv2C までの全機能に加えて，管理セキュリティ機能が大幅に強化されています。ネットワーク上を流れる SNMP パケットを認証・暗号化することによって，SNMPv2C でのコミュニティ名と SNMP マネージャの IP アドレスの組み合わせによるセキュリティ機能では実現できなかった，盗聴，なりすまし，改ざん，再送などのネットワーク上の危険から SNMP パケットを守ることができます。

(a) SNMP エンティティ

SNMPv3 では，SNMP マネージャおよび SNMP エージェントを「SNMP エンティティ」と総称します。本装置の SNMPv3 は，SNMP エージェントに相当する SNMP エンティティをサポートしています。

(b) SNMP エンジン

SNMP エンジンは認証，および暗号化したメッセージ送受信と管理オブジェクトへのアクセス制御のためのサービスを提供します。SNMP エンティティとは 1 対 1 の関係です。SNMP エンジンは，同一管理ドメイン内でユニークな SNMP エンジン ID により識別されます。

(c) ユーザ認証とプライバシー機能

SNMPv1，SNMPv2C でのコミュニティ名による認証に対して，SNMPv3 ではユーザ認証を行います。また，SNMPv1，SNMPv2C にはなかったプライバシー機能（暗号化，復号化）も SNMPv3 でサポートされています。ユーザ認証とプライバシー機能は，ユーザ単位に設定できます。

本装置では，ユーザ認証プロトコルとして次の二つプロトコルをサポートしています。

- HMAC-MD5-96（メッセージダイジェストアルゴリズムを使用した認証プロトコル。128 ビットのダイジェストのうち，最初の 96 ビットを使用する。秘密鍵は 16 オクテット）
- HMAC-SHA-96（SHA メッセージダイジェストアルゴリズムを使用した認証プロトコル。160 ビットの SHA ダイジェストのうち，最初の 96 ビットを使用する。秘密鍵は 20 オクテット）

プライバシープロトコルとして次のプロトコルをサポートしています。

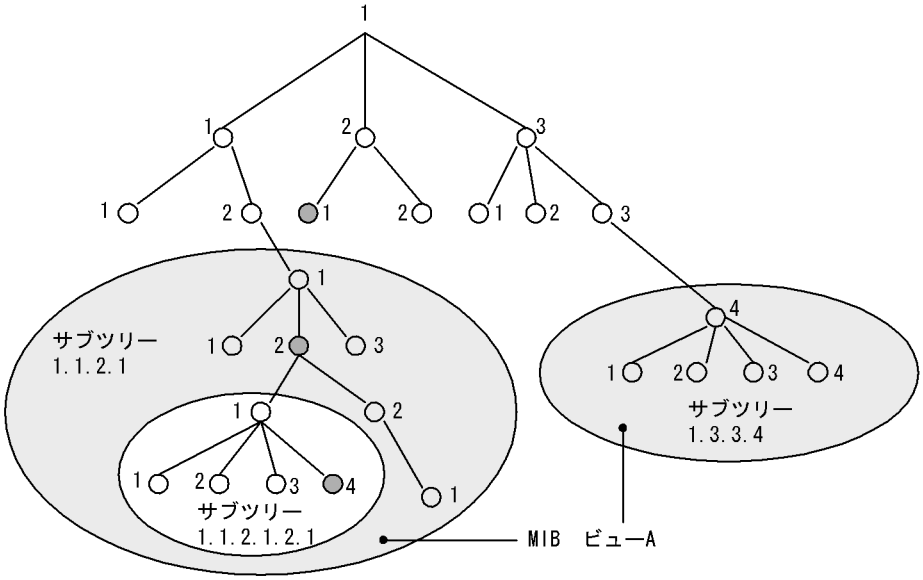
- CBC-DES（Cipher Block Chaining - Data Encryption Standard。共通鍵暗号アルゴリズムである DES（56 ビット鍵）を，CBC モードで強力にした暗号化プロトコル）

(d) MIB ビューによるアクセス制御

SNMPv3 では，ユーザ単位に，アクセスできる MIB オブジェクトの集合を設定できます。この MIB オブジェクトの集合を MIB ビューと呼びます。MIB ビューは，MIB のオブジェクト ID のツリーを表すビューサブツリーを集約することによって表現されます。集約する際には，ビューサブツリーごとに included（MIB ビューに含む），または excluded（MIB ビューから除外する）を選択できます。MIB ビューは，ユーザ単位に，Read ビュー，Write ビュー，Notify ビューとして設定できます。

次に，MIB ビューの例を示します。MIB ビューは，「図 21-5　MIB ビューの例」に示すような MIB ツリーの一部である MIB サブツリーをまとめて設定します。オブジェクト ID 1.1.2.1.2 は，サブツリー 1.1.2.1 に含まれるので，MIB ビュー A でアクセスできます。しかし，オブジェクト ID 1.2.1 は，どちらのサブツリーにも含まれないので，アクセスできません。また，オブジェクト ID 1.1.2.1.2.1.4 は，サブツリー 1.1.2.1.2.1 がビュー A から除外されているためアクセスできません。

図 21-5　MIB ビューの例



コンフィグレーションの内容
```
ViewA  1.1.2.1       included
       1.3.3.4       included
       1.1.2.1.2.1 excluded
```

21.1.2　MIB 概説

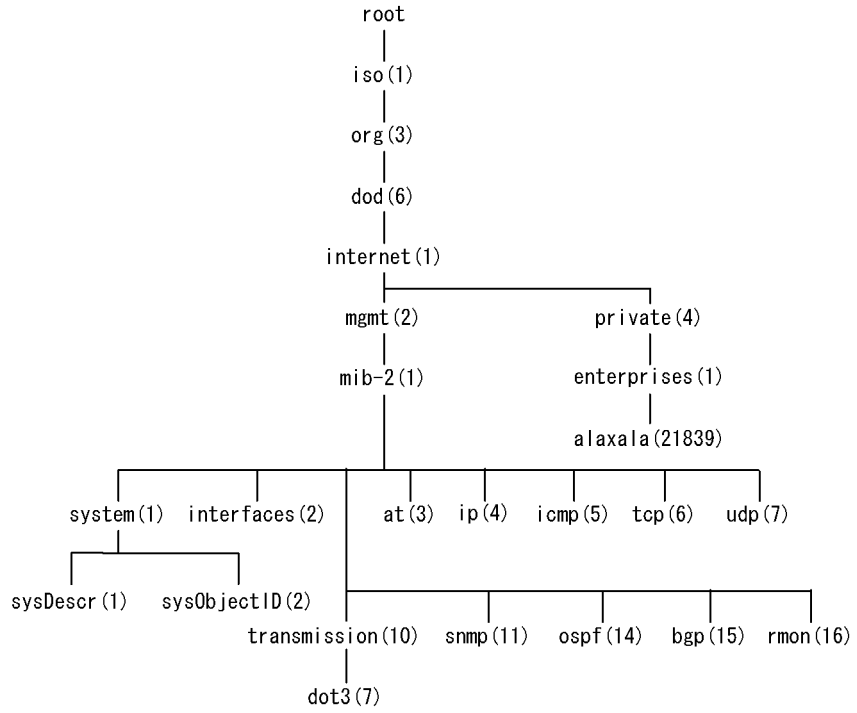
装置が管理し，SNMP マネージャに提供する MIB は，RFC で規定されたものと，装置の開発ベンダーが独自に用意する情報の 2 種類があります。

RFC で規定された MIB を**標準** MIB と呼びます。標準 MIB は規格化されているため提供情報の内容の差はあまりありません。装置の開発ベンダーが独自に用意する MIB を**プライベート** MIB と呼び，装置によって内容が異なります。ただし，MIB のオペレーション（情報の採取・設定など）は，標準 MIB，プライベート MIB で共通です。オペレーションは，装置と目的の MIB 情報を指定するだけです。装置は IP アドレスで，MIB 情報はオブジェクト ID で指定します。

(1) MIB 構造

MIB の構造はツリー構造になっています。MIB はツリー構造のため，各ノードを識別するために番号を付けて表す決まりになっています。root から各ノードの数字を順番にたどって番号を付けることで個々の MIB 情報を一意に識別できます。この番号列をオブジェクト ID と呼びます。オブジェクト ID は root から下位のオブジェクトグループ番号をドットで区切って表現します。例えば，sysDescr という MIB をオブジェクト ID で示すと 1.3.6.1.2.1.1.1 になります。MIB ツリーの構造例を次の図に示します。

図 21-6 MIB ツリーの構造例



(2) MIB オブジェクトの表し方

オブジェクト ID は数字と.（ドット）（例：1.3.6.1.2.1.1.1）で表現します。しかし，数字の羅列ではわかりにくいため，マネージャによっては，sysDescr というニーモニックで指定できるものもあります。ニーモニックで指定する場合，SNMP マネージャがどの MIB のニーモニックを使えるか確認してから使用してください。また，本装置の SNMP コマンドで使用できるニーモニックについては，snmp lookup コマンドを実行することで確認できます。

(3) インデックス

MIB を指定するときのオブジェクト ID を使用しますが，一つの MIB に一つの意味だけある場合と一つの MIB に複数の情報がある場合があります。MIB を特定するためにはインデックス（INDEX）を使用します。インデックスは，オブジェクト ID の後ろに数字を付加して表し，何番目の情報かなどを示すために使用します。

一つの MIB に一つの意味だけがある場合，MIB のオブジェクト ID に ".0" を付加して表します。一つの MIB に複数の情報がある場合，MIB のオブジェクト ID の後ろに数字を付加して何番目の情報であるか表します。例えば，インタフェースのタイプを示す MIB に ifType（1.3.6.1.2.1.2.2.1.2）があります。本装置には複数のインタフェースがあります。特定のインタフェースのタイプを調べるには，"2 番目のインタフェースのタイプ " というように具体的に指定する必要があります。MIB で指定するときは，2 番目を示

すインデックス .2 を MIB の最後に付加して ifType.2（1.3.6.1.2.1.2.2.1.2.2）と表します。

インデックスの表し方は，各 MIB によって異なります。RFC などの MIB の定義で，INDEX{ xxxxx,yyyyy,zzzzzz }となっている MIB のエントリは，xxxxx と yyyyy と zzzzzz をインデックスに持ちます。それぞれの MIB について，どのようなインデックスを取るか確認して MIB のオペレーションを行ってください。

(4) 本装置のサポート MIB

本装置では，装置の状態，インタフェースの統計情報，装置の機器情報など，管理に必要な MIB を提供しています。なお，プライベート MIB の定義（ASN.1）ファイルは，ソフトウェアとともに提供します。

各 MIB の詳細については，マニュアル「MIB レファレンス」を参照してください。

21.1.3 SNMPv1，SNMPv2C オペレーション

管理データ（MIB:management information base）の収集や設定を行うため，SNMP では次に示す 4 種類のオペレーションがあります。

- GetRequest　　：指定した MIB の情報を取り出します。
- GetNextRequest：指定した次の MIB の情報を取り出します。
- GetBulkRequest：GetNextRequest の拡張版です。
- SetRequest　　：指定した MIB に値を設定します。

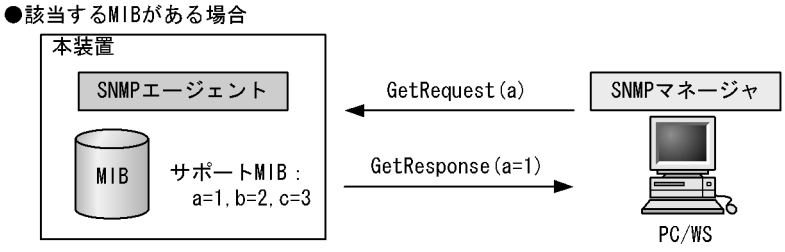
各オペレーションは SNMP マネージャから装置（SNMP エージェント）に対して行われます。各オペレーションについて説明します。

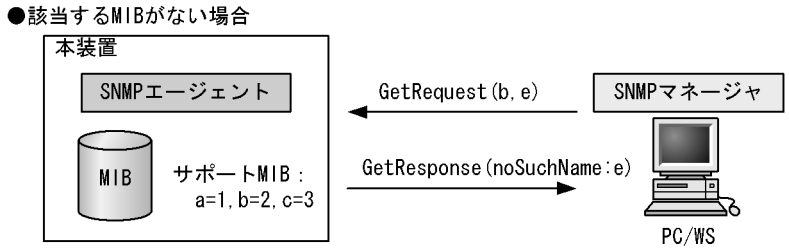
(1) GetRequest オペレーション

GetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して MIB の情報を取り出すときに使用します。このオペレーションでは，一つまたは複数 MIB を指定できます。

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

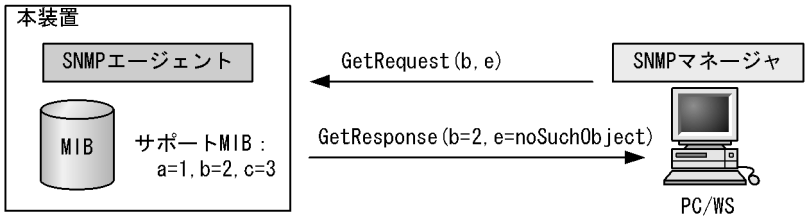
図 21-7　GetRequest オペレーション





SNMPv2C では，装置が該当する MIB を保持していない場合は，GetResponse オペレーションで MIB 値に noSuchObject を応答します。SNMPv2C の場合の GetRequest オペレーションを次の図に示します。

図 21-8　GetRequest オペレーション（SNMPv2C）

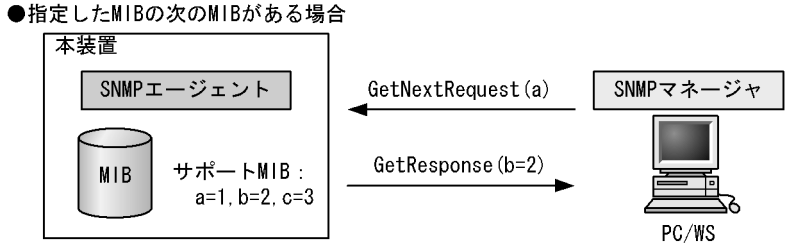


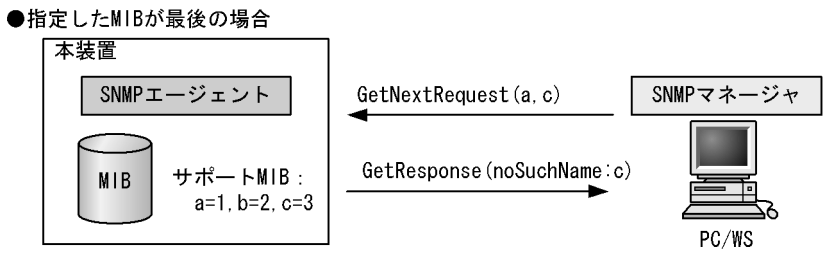
(2) GetNextRequest オペレーション

GetNextRequest オペレーションは，GetRequest オペレーションに似たオペレーションです。GetRequest オペレーションは，指定した MIB の読み出しに使用しますが，GetNextRequest オペレーションは，指定した MIB の次の MIB を取り出すときに使用します。このオペレーションも一つまたは複数の MIB を指定できます。

装置が指定した次の MIB を保持している場合は，GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合は，GetResponse で noSuchName を応答します。GetNextRequest オペレーションを次の図に示します。

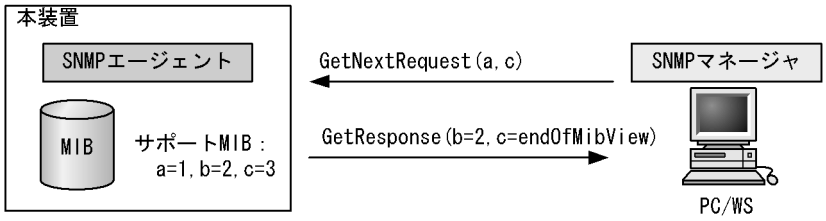
図 21-9　GetNextRequest オペレーション





SNMPv2C の場合，指定した MIB が最後の場合は GetResponse で MIB 値に endOfMibView を応答します。SNMPv2C の場合の GetNextRequest オペレーションを次の図に示します。

図 21-10 GetNextRequest オペレーション（SNMPv2C）

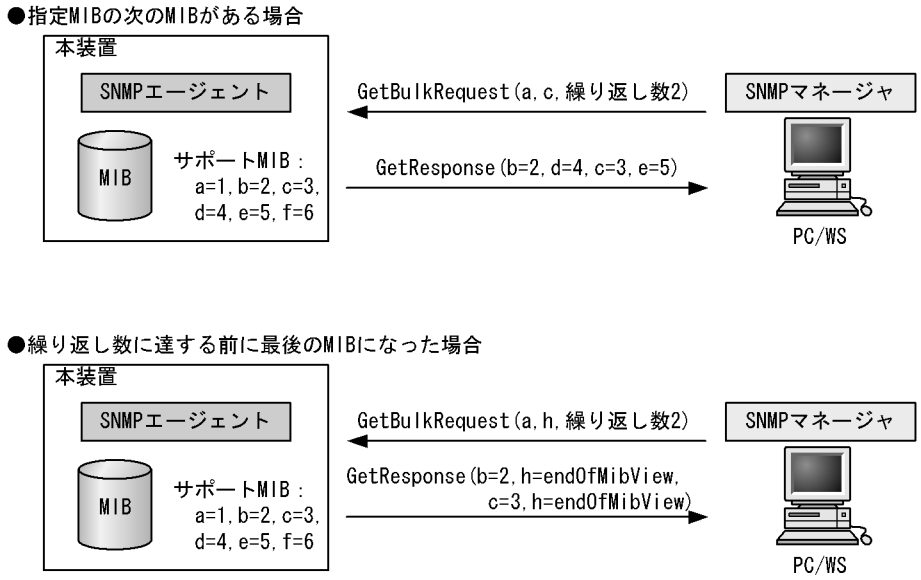


(3) GetBulkRequest オペレーション

GetBulkRequest オペレーションは，GetNextRequest オペレーションを拡張したオペレーションです。このオペレーションでは繰り返し回数を設定し，指定した MIB の次の項目から指定した繰り返し回数個分の MIB を取得できます。このオペレーションも，一つまたは複数の MIB を指定できます。

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

図 21-11 GetBulkRequest オペレーション

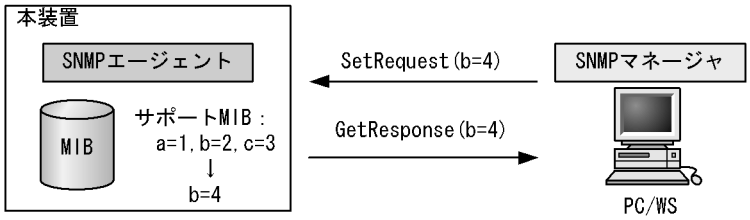


(4) SetRequest オペレーション

SetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して行うオペレーションという点で GetRequest，GetNextRequest，GetBulkRequest オペレーションと似ていますが，値の設定方法が異なります。

SetRequest オペレーションでは，設定する値と MIB を指定します。値を設定すると，GetResponse オペレーションで MIB と設定値を応答します。SetRequest オペレーションを次の図に示します。

図 21-12 SetRequest オペレーション



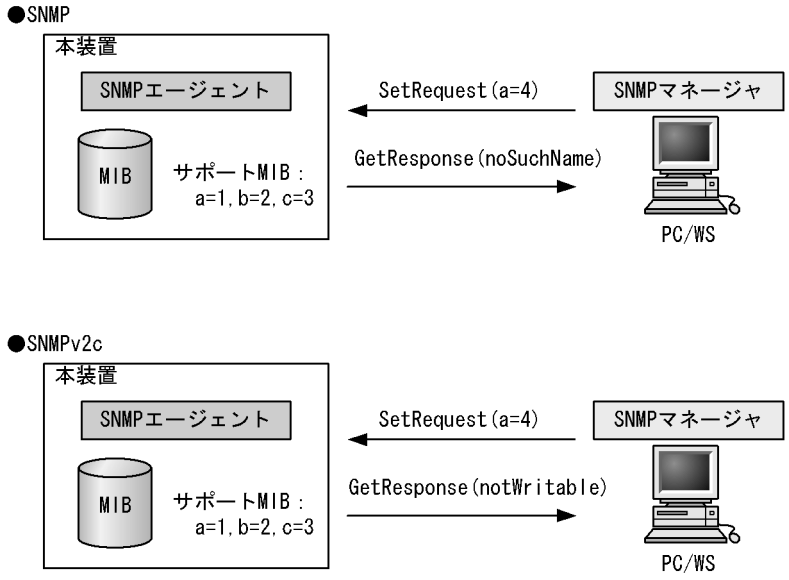
(a) MIB を設定できない場合の応答

MIB を設定できないケースは，次に示す 3 とおりです。

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

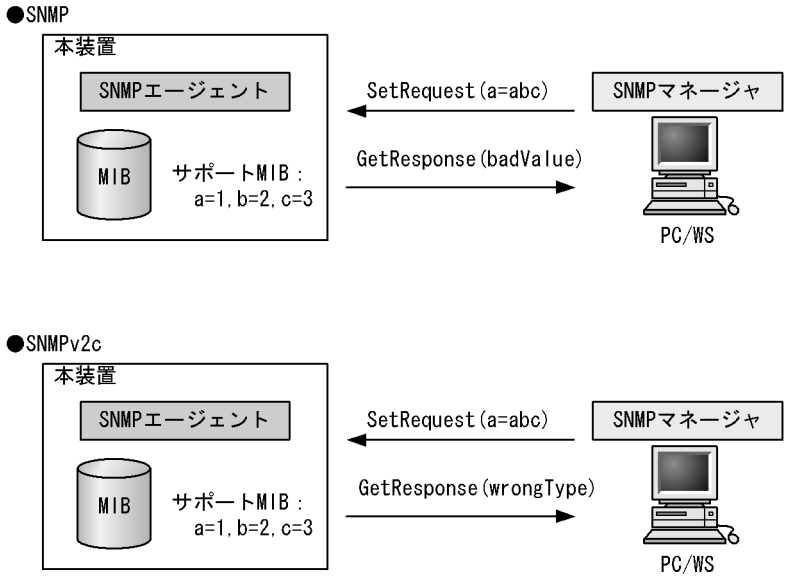
各ケースによって，応答が異なります。MIB が読み出し専用の場合，noSuchName の GetResponse 応答をします。SNMPv2C の場合，MIB が読み出し専用のときは notWritable の GetResponse 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 21-13 MIB 変数が読み出し専用の場合の SetRequest オペレーション



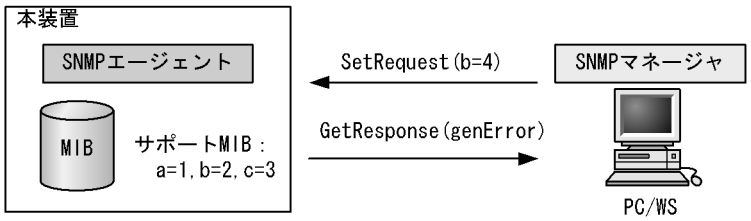
設定値のタイプが正しくない場合，badValue の GetResponse 応答をします。SNMPv2C の場合，設定値のタイプが正しくないときは wrongType の GetResponse 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 21-14 設定値のタイプが正しくない場合の SetRequest オペレーション例



装置の状態によって設定できない場合，genError を応答します。例えば，装置内で値を設定しようとしたときに，装置内部で設定タイムアウトを検出した場合などがこれに当てはまります。装置の状態によって設定できない場合の SetRequest オペレーションを次の図に示します。

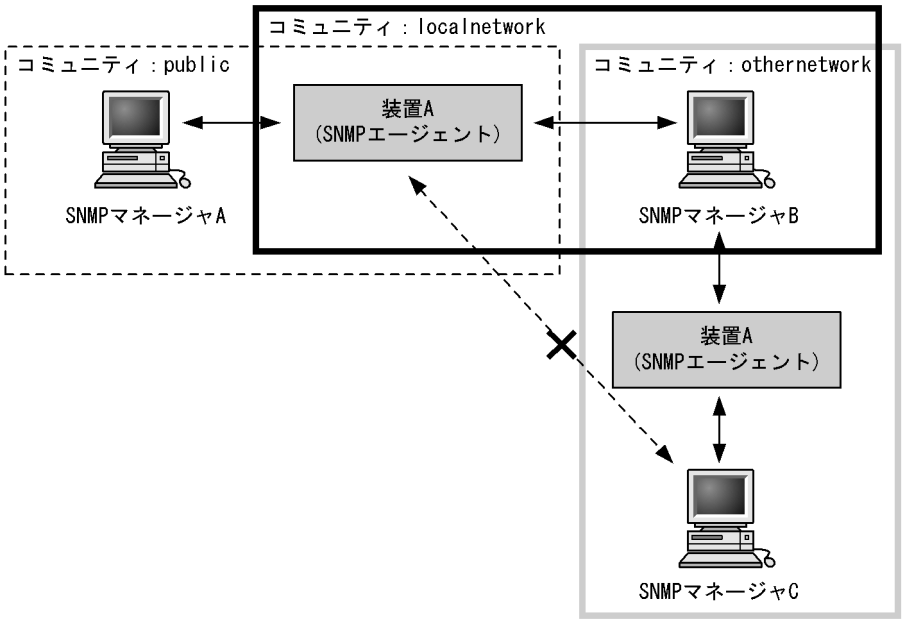
図 21-15 装置の状態によって設定できない場合の SetRequest オペレーション



(5) コミュニティによるオペレーション制限

SNMPv1 および SNMPv2C では，オペレーションを実行する SNMP マネージャを限定するため，コミュニティという概念があります。コミュニティはオペレーションを実行する SNMP マネージャと SNMP エージェントを一つのグループとして割り当てる名称です。MIB に対してオペレーションする場合は，SNMP マネージャと SNMP エージェントは，同一のグループ（コミュニティ）に属する必要があります。コミュニティによるオペレーションを次の図に示します。

図 21-16 コミュニティによるオペレーション



装置 A はコミュニティ（public）およびコミュニティ（localnetwork）に属しています。コミュニティ（othernetwork）には属していません。この場合，装置 A はコミュニティ（public）およびコミュニティ（localnetwork）の SNMP マネージャ A，B から MIB のオペレーションを受け付けますが，コミュニティ（othernetwork）の SNMP マネージャ C からのオペレーションは受け付けません。

（6） IP アドレスによるオペレーション制限

本装置では，セキュリティを考慮し，アクセスリストを使用することでコミュニティと SNMP マネージャの IP アドレスの組み合わせが合わないときは MIB のオペレーションを受け付けないようにできます。本装置で SNMPv1 および SNMPv2C を使用するときは，コミュニティをコンフィグレーションコマンドで登録する必要があります。なお，コミュニティは文字列で設定します。また，一般的にコミュニティ名称は，public を使用している場合が多いです。

（7） SNMP オペレーションのエラーステータスコード

オペレーションでエラーが発生した場合，SNMP エージェントはエラーステータスにエラーコードを設定し，何番目の MIB 情報でエラーが発生したかをエラー位置番号に設定した GetResponse オペレーションの応答を返します。オペレーションの結果が正常なら，エラーステータスにエラーなしのコードを設定し，MIB 情報内にオペレーションした MIB 情報を設定した GetResponse オペレーションの応答を返します。エラーステータスコードを次の表に示します。

表 21-1 エラーステータスコード

エラーステータス	コード	内容
noError	0	エラーはありません。
tooBig	1	データサイズが大きく PDU に値を設定できません。
noSuchName	2	指定 MIB がない，または書き込みできませんでした。
badValue	3	設定値が不正です。
readOnly	4	書き込みできませんでした（本装置では，応答することはありません）。

エラーステータス	コード	内容
genError	5	その他のエラーが発生しました。
noAccess	6	アクセスできない MIB に対して set を行おうとしました。
wrongType	7	MIB で必要なタイプと異なるタイプが指定されました。
wrongLength	8	MIB で必要なデータ長と異なる長さが指定されました。
wrongEncoding	9	ASN.1 符号が不正でした。
wrongValue	10	MIB 値が不正でした。
noCreation	11	該当する MIB が存在しません。
inconsistentValue	12	現在何か理由があって値が設定できません。
resourceUnavailable	13	値の設定のためにリソースが必要ですが，リソースが利用できません。
commitFailed	14	値の更新に失敗しました。
undoFailed	15	値の更新に失敗したときに，更新された値を元に戻すのに失敗しました。
notWritable	17	セットできません。
inconsistentName	18	該当する MIB が存在しないため，現在は作成できません。

21.1.4 SNMPv3 オペレーション

管理データ（MIB:management information base）の収集や設定を行うため，SNMP では次に示す四種類のオペレーションがあります。

- GetRequest　　：指定した MIB の情報を取り出します。
- GetNextRequest：指定した次の MIB の情報を取り出します。
- GetBulkRequest：GetNextRequest の拡張版です。
- SetRequest　　：指定した MIB に値を設定します。

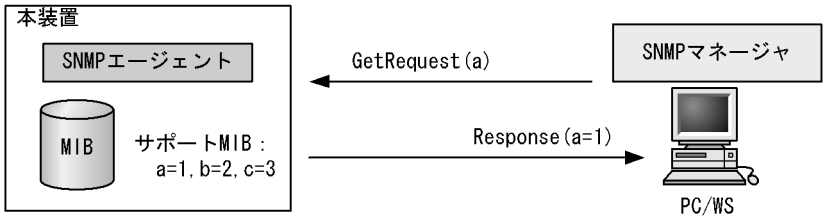
各オペレーションは SNMP マネージャから装置（SNMP エージェント）に対して行われます。各オペレーションについて説明します。

（1） GetRequest オペレーション

GetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して MIB の情報を取り出すときに使用します。このオペレーションでは，一つまたは複数の MIB を指定できます。装置が該当する MIB を保持している場合，Response オペレーションで MIB 情報を応答します。

GetRequest オペレーションを次の図に示します。

図 21-17　GetRequest オペレーション

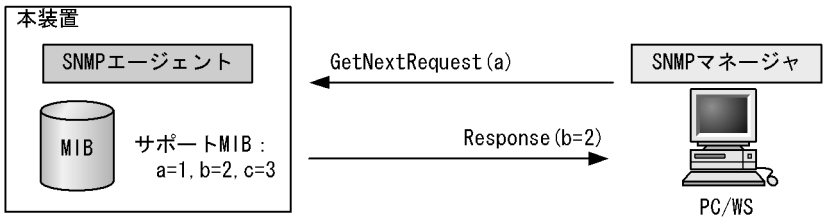


(2) GetNextRequest オペレーション

GetNextRequest オペレーションは，GetRequest オペレーションに似たオペレーションです。GetRequest オペレーションが指定した MIB の読み出しに使用するのに対し，GetNextRequest オペレーションは指定した MIB の次の MIB を取り出すときに使用します。このオペレーションも一つまたは複数の MIB を指定できます。

GetNextRequest オペレーションを次の図に示します。

図 21-18 GetNextRequest オペレーション

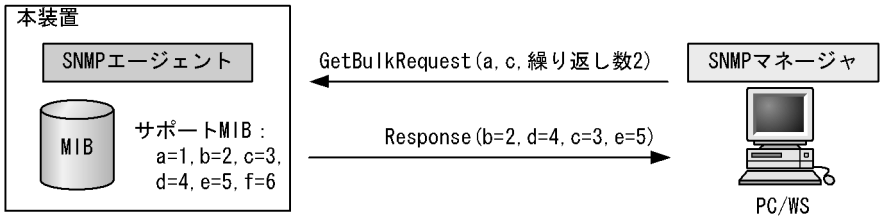


(3) GetBulkRequest オペレーション

GetBulkRequest オペレーションは，GetNextRequest オペレーションを拡張したオペレーションです。このオペレーションでは繰り返し回数を設定し，指定した MIB の次の項目から指定した繰り返し回数個分の MIB を取得できます。このオペレーションも，一つまたは複数の MIB を指定できます。

GetBulkRequest オペレーションを次の図に示します。

図 21-19 GetBulkRequest オペレーション



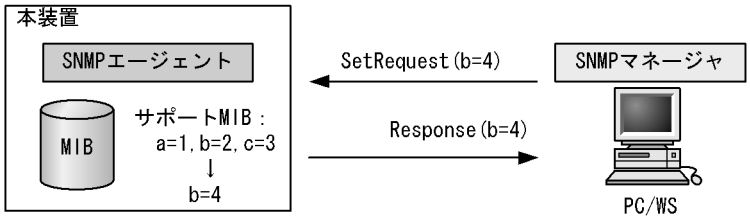
(4) SetRequest オペレーション

SetRequest オペレーションは，SNMP マネージャから装置（エージェント機能）に対して行うオペレーションという点で GetRequest，GetNextRequest，GetBulkRequest オペレーションと似ていますが，値の設定方法が異なります。

SetRequest オペレーションでは，設定する値と MIB を指定します。値を設定すると，Response オペレーションで MIB と設定値を応答します。

SetRequest オペレーションを次の図に示します。

図 21-20 SetRequest オペレーション



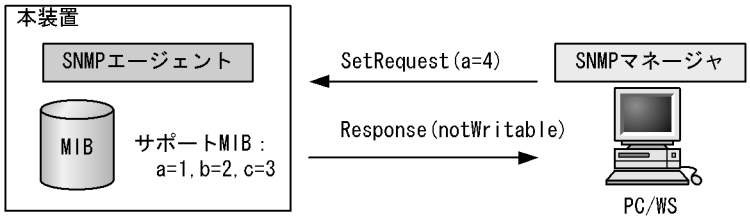
(a) MIB を設定できない場合の応答

MIB を設定できないケースは，次に示す 3 とおりです。

- MIB が読み出し専用の場合
- 設定値が正しくない場合
- 装置の状態によって設定できない場合

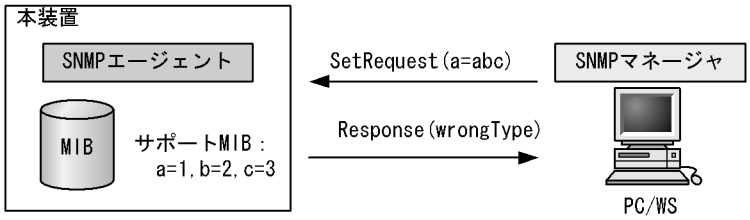
各ケースによって，応答が異なります。MIB が読み出し専用のときは notWritable の Response 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 21-21 MIB 変数が読み出し専用の場合の SetRequest オペレーション



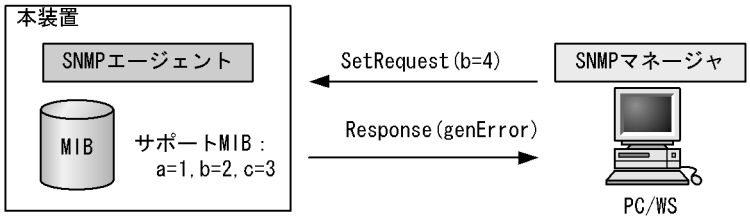
設定値のタイプが正しくないときは wrongType の Response 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 21-22 設定値のタイプが正しくない場合の SetRequest オペレーション例



装置の状態によって設定できない場合，genError を応答します。例えば，装置内で値を設定しようとしたときに，装置内部で設定タイムアウトを検出した場合などがこれに当てはまります。装置の状態によって設定できない場合の SetRequest オペレーションを次の図に示します。

図 21-23 装置の状態によって設定できない場合の SetRequest オペレーション



(5) SNMPv3 でのオペレーション制限

SNMPv1 および SNMPv2C ではコミュニティと SNMP マネージャの IP アドレスの組み合わせによって確認が行われるのに対し，SNMPv3 ではユーザ認証と MIB ビューによって MIB のオペレーションを制限します。本装置で SNMPv3 を使用するときは，SNMP セキュリティユーザ，MIB ビューおよびセキュリティグループをコンフィグレーションコマンドで登録する必要があります。また，トラップを送信するには，SNMP セキュリティユーザ，MIB ビュー，セキュリティグループ，およびトラップ送信 SNMP マネージャをコンフィグレーションコマンドで登録する必要があります。

(6) SNMPv3 オペレーションのエラーステータスコード

オペレーションの結果エラーが発生した場合，SNMP エージェントはエラーステータスにエラーコードを設定し，何番目の MIB 情報でエラーが発生したかをエラー位置番号に設定した Response オペレーションの応答を返します。オペレーションの結果が正常であれば，エラーステータスにエラーなしのコードを設定し，MIB 情報内にオペレーションした MIB 情報を設定した Response オペレーションの応答を返します。エラーステータスコードを次の表に示します。

表 21-2 エラーステータスコード

エラーステータス	コード	内容
noError	0	エラーはありません。
tooBig	1	データサイズが大きく PDU に値を設定できません。
noSuchName	2	指定 MIB がない，または書き込みできませんでした。
badValue	3	設定値が不正です。
readOnly	4	書き込みできませんでした（本装置では，応答することはありません）。
genError	5	その他のエラーが発生しました。
noAccess	6	アクセスできない MIB に対して set を行おうとしました。
wrongType	7	MIB で必要なタイプと異なるタイプが指定されました。
wrongLength	8	MIB で必要なデータ長と異なる長さが指定されました。
wrongEncoding	9	ASN.1 符号が不正でした。
wrongValue	10	MIB 値が不正でした。
noCreation	11	該当する MIB が存在しません。
inconsistentValue	12	現在何か理由があって値が設定できません。
resourceUnavailable	13	値の設定のためにリソースが必要ですが，リソースが利用できません。
commitFailed	14	値の更新に失敗しました。
undoFailed	15	値の更新に失敗したときに，更新された値を元に戻すのに失敗しました。
authorizationError	16	認証に失敗しました。
notWritable	17	セットできません。

エラーステータス	コード	内容
inconsistentName	18	該当する MIB が存在しないため，現在は作成できません。

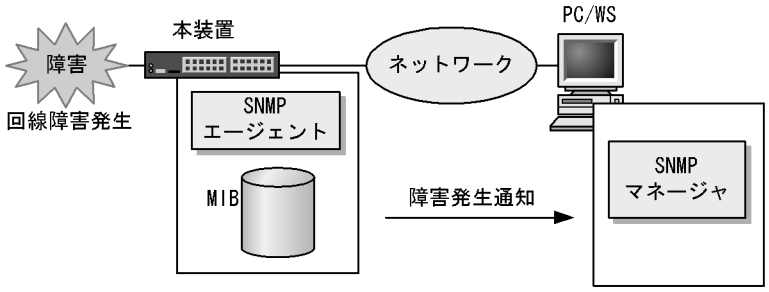
21.1.5 トラップ

(1) トラップ概説

SNMP エージェントは**トラップ（Trap）**と呼ばれるイベント通知（主に障害発生の情報やログ情報など）機能があります。トラップは重要なイベントを SNMP エージェントから SNMP マネージャに非同期に通知する機能です。SNMP マネージャは，トラップを受信することで定期的に装置の状態変化を検知できます。この通知を基に，装置内の MIB を取得して，さらに詳細な情報を得ることができます。

なお，トラップは UDP を使用しているため，装置から SNMP マネージャに対するトラップの到達が確認できません。そのため，ネットワークの輻輳などによってトラップがマネージャに到達しない場合があります。トラップの例を次の図に示します。

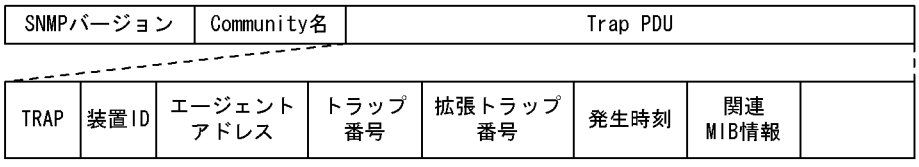
図 21-24 トラップの例



(2) トラップフォーマット

トラップフレームには，どの IP アドレスの装置で，いつ，何が発生したかを示す情報を含みます。トラップフォーマットを次の図に示します。

図 21-25 トラップフォーマット



装置ID　：装置の識別ID（通常MIB-IIのsysObjectIDの値が設定される）
エージェントアドレス：トラップが発生した装置のIPアドレス
トラップ番号　：トラップの種別を示す識別番号
拡張トラップ番号　：トラップ番号の補足をするための番号
発生時刻　：トラップが発生した時間（装置が起動してからの経過時間）
関連MIB情報　：このトラップに関連するMIB情報

21.1.6 RMON MIB

RMON（Remote Network Monitoring）とは，イーサネット統計情報を提供する機能，収集した統計情報の閾値チェックを行ってイベントを発生させる機能，パケットをキャプチャする機能などを持ちます。この RMON は RFC1757 で規定されています。

RMON MIB のうち，statistics，history，alarm，event の各グループについて概要を説明します。

（1） statistics グループ

監視対象のサブネットワークについての，基本的な統計情報を収集します。例えば，サブネットワーク中の総パケット数，ブロードキャストパケットのような各種類ごとのパケット数，CRC エラー，コリジョンエラーなどのエラー数などです。statistics グループを使うと，サブネットワークのトラフィック状況や回線状態などの統計情報を取得できます。

（2） history グループ

statistics グループで収集する情報とほぼ同じ統計情報をサンプリングし，来歴情報として保持できます。

history グループには historyControlTable という制御テーブルと，etherHistoryTable というデータテーブルがあります。historyControlTable はサンプリング間隔や来歴記録数の設定を行うための MIB です。

etherHistoryTable は，サンプリングした統計情報の来歴記録の MIB です。history グループは，一定期間の統計情報を装置内で保持しています。このため，SNMP マネージャなどが定期的にポーリングして統計情報を収集するのと比較して，ネットワークに負荷をかけることが少なく，連続した一定期間の統計情報を取得できます。

（3） alarm グループ

監視対象とする MIB のチェック間隔，閾値などを設定して，その MIB が閾値に達したときにログを記録したり，SNMP マネージャにトラップを発行したりすることを指定する MIB です。この alarm グループを使用するときは，event グループも設定する必要があります。

alarm グループによる MIB 監視には，MIB 値の差分（変動）と閾値を比較する delta **方式**と，MIB 値と閾値を直接比較する absolute **方式**があります。

delta 方式による閾値チェックでは，例えば，CPU 使用率の変動が 50% 以上あったときに，ログを収集したり，SNMP マネージャにトラップを発行したりできます。absolute 方式による閾値チェックでは，例えば，CPU の使用率が 80% に達したときに，ログを収集したり，SNMP マネージャにトラップを発行したりできます。

本装置では，閾値をチェックするタイミングによる検出漏れをできるだけ防止するために，alarmInterval（MIB 値を監視する時間間隔（秒）を表す MIB）の間に複数回チェックします。alarmInterval ごとの閾値チェック回数を次の表に示します。

表 21-3　alarmInterval ごとの閾値チェック回数

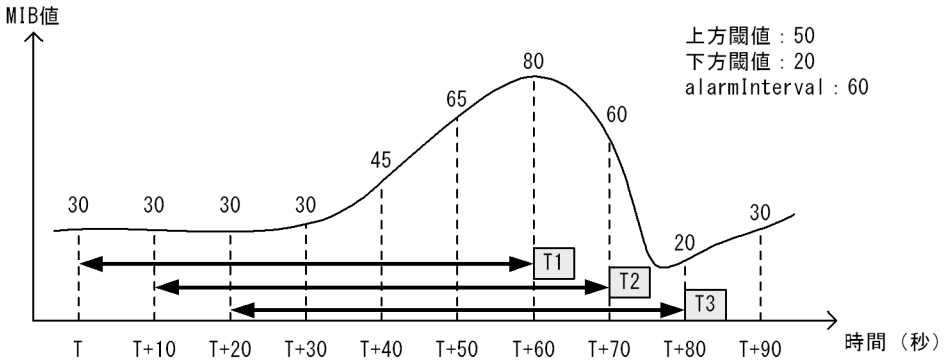
alarmInterval（秒）	閾値チェック回数
1	1
2 ～ 5	2
6 ～ 10	3
11 ～ 20	4
21 ～ 50	5
51 ～ 100	6
101 ～ 200	7
201 ～ 400	8
401 ～ 800	9

alarmInterval（秒）	閾値チェック回数
801 ～ 1300	10
1301 ～ 2000	11
2001 ～ 4294967295	12

閾値のチェックは，およそ alarmInterval を閾値チェック回数で割った秒数ごとに行います。例えば，alarmInterval が 60（秒）の場合，閾値チェック回数は 6 回になるため，10 秒に 1 回のタイミングで閾値をチェックします。

上方閾値を 50，下方閾値を 20，alarmInterval を 60 として，CPU 使用率の MIB 値を delta 方式で監視した場合の例を次の図に示します。

図 21-26　delta 方式による MIB 監視例



T1

閾値と比較する値が 50（T+60（秒）の MIB 値 80 － T（秒）の MIB 値 30）のため，上方閾値以上を検出

T2

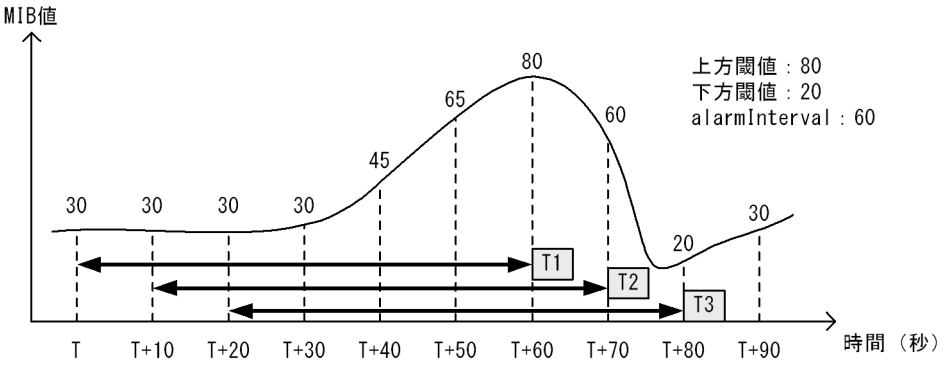
閾値と比較する値が 30（T+70（秒）の MIB 値 60 － T+10（秒）の MIB 値 30）のため，閾値検出なし

T3

閾値と比較する値が -10（T+80（秒）の MIB 値 20 － T+20（秒）の MIB 値 30）のため，下方閾値以下を検出

上方閾値を 80，下方閾値を 20，alarmInterval を 60 として，CPU 使用率の MIB 値を absolute 方式で監視した場合の例を次の図に示します。

図 21-27　absolute 方式による MIB 監視例



T1

閾値と比較する値が 80（T+60（秒）の MIB 値）のため，上方閾値以上を検出

T2

閾値と比較する値が 60（T+70（秒）の MIB 値）のため，閾値検出なし

T3

閾値と比較する値が 20（T+80（秒）の MIB 値）のため，下方閾値以下を検出

（4）event グループ

event グループには alarm グループで設定した MIB の閾値を超えたときの動作を指定する eventTable グループ MIB と閾値を超えたときにログを記録する logTable グループ MIB があります。

eventTable グループ MIB は，閾値に達したときにログを記録するのか，SNMP マネージャにトラップを発行するのか，またはその両方するか何もしないかを設定するための MIB です。

logTable グループ MIB は，eventTable グループ MIB でログの記録を指定したときに，装置内にログを記録します。装置内のログのエントリ数は決まっているので，エントリをオーバーした場合，新しいログ情報の追加によって，古いログ情報が消去されていきます。定期的に SNMP マネージャに記録を退避しないと，前のログが消されてしまう可能性がありますので注意してください。

21.1.7　SNMP マネージャとの接続時の注意事項

（1）MIB 情報収集周期のチューニング

SNMP マネージャは，ネットワーク上の新しい装置を検出したり，トラフィック状況を監視したりするため，SNMP エージェントサポート機器から定期的に MIB を取得します。この定期的な MIB 取得の間隔が短いと，ネットワーク機器やネットワークに負荷が掛かります。また，装置の状態や構成などによって，MIB 取得時にマネージャ側でタイムアウトが発生するおそれがあります。特に，次に示すケースでは応答タイムアウトの発生するおそれが高まります。

- 接続 SNMP マネージャ数が多い場合
  本装置に SNMP マネージャが多数接続され，MIB 情報の収集が集中した場合。
- SNMP イベントが同時に多数発生している場合
  本装置から大量にトラップが発行されるような状態のときに，MIB を取得した場合や，本装置から発行されたトラップに基づいて，並行して MIB を取得した場合。

応答タイムアウトが頻発する場合は，SNMP マネージャのポーリング周期や応答監視タイマ値をチューニ

ングしてください。代表的な SNMP マネージャのチューニングパラメータには，次の三つがあります。

- ポーリング周期
- 応答監視タイマ
- 応答監視タイムアウト時のリトライ回数

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

SNMP/RMON 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 21-4 コンフィグレーションコマンド一覧

コマンド名	説明
hostname	本装置のホスト名称を設定します。本設定は RFC1213 の sysName に対応します。
rmon alarm	RMON（RFC1757）アラームグループの制御情報を設定します。
rmon collection history	RMON（RFC1757）イーサネットの統計来歴の制御情報を設定します。
rmon event	RMON（RFC1757）イベントグループの制御情報を設定します。
snmp-server community	SNMP コミュニティに対するアクセスリストを設定します。
snmp-server contact	本装置の連絡先などを設定します。本設定は RFC1213 の sysContact に対応します。
snmp-server engineID local	SNMP エンジン ID 情報を設定します。
snmp-server group	SNMP セキュリティグループ情報を設定します。
snmp-server host	トラップを送信するネットワーク管理装置（SNMP マネージャ）を登録します。
snmp-server location	本装置を設置する場所の名称を設定します。本設定は RFC1213 の sysLocation に対応します。
snmp-server traps	トラップの発行契機を設定します。
snmp-server user	SNMP セキュリティユーザ情報を設定します。
snmp-server view	MIB ビュー情報を設定します。
snmp trap link-status	回線がリンクアップまたはダウンした場合に，トラップ（SNMP link down および up Trap）の送信を抑止します。

21.2.2 SNMPv1，SNMPv2C による MIB アクセス許可の設定

[設定のポイント]

SNMP マネージャから本装置の MIB へのアクセスを許可するための設定をします。

[コマンドによる設定]

1. **(config)# access-list 1 permit 128.1.1.2 0.0.0.0**
   IP アドレス 128.1.1.2 からのアクセスを許可するアクセスリストの設定を行います。

2. **(config)# snmp-server community "NETWORK" ro 1**
   SNMP マネージャのコミュニティに対する MIB アクセスモードおよび適用するアクセスリストを設定します。
   - コミュニティ名：NETWORK
   - アクセスリスト：1
   - アクセスモード：read only

21.2.3 SNMPv3 による MIB アクセス許可の設定

[設定のポイント]

SNMPv3 で MIB にアクセスするために，アクセスを許可する MIB オブジェクトの集合を MIB ビューとして設定し，ユーザ認証とプライバシー機能の情報を SNMP セキュリティユーザとして設定します。また，MIB ビューと SNMP セキュリティユーザを関連づけるために，SNMP セキュリティグループを設定します。

[コマンドによる設定]

1. **(config)# snmp-server view "READ_VIEW" 1.3.6.1 included**
   (config)# snmp-server view "READ_VIEW" 1.3.6.1.6.3 excluded
   (config)# snmp-server view "WRITE_VIEW" 1.3.6.1.2.1.1 included
   MIB ビューを設定します。
   - ビュー名 READ_VIEW に internet グループ MIB（サブツリー：1.3.6.1）を登録します。
   - ビュー名 READ_VIEW から snmpModules グループ MIB（サブツリー：1.3.6.1.6.3）を対象外にします。
   - ビュー名 WRITE_VIEW に system グループ MIB（サブツリー：1.3.6.1.2.1.1）を登録します。

2. **(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789"**
   SNMP セキュリティユーザを設定します。
   - SNMP セキュリティユーザ名：ADMIN
   - SNMP セキュリティグループ名：ADMIN_GROUP
   - 認証プロトコル：HMAC-MD5
   - 認証パスワード：ABC*_1234
   - 暗号化プロトコル：CBC-DES
   - 暗号化パスワード：XYZ/+6789

3. **(config)# snmp-server group "ADMIN_GROUP" v3 priv read "READ_VIEW" write "WRITE_VIEW"**
   SNMP セキュリティグループを設定します。
   - SNMP セキュリティグループ名：ADMIN_GROUP
   - セキュリティレベル：認証あり，暗号化あり
   - Read ビュー名：READ_VIEW
   - Write ビュー名：WRITE_VIEW

21.2.4 SNMPv1，SNMPv2C によるトラップ送信の設定

[設定のポイント]

トラップを発行する SNMP マネージャを登録します。

[コマンドによる設定]

1. **(config)# snmp-server host 128.1.1.2 traps "NETWORK" version 1 snmp**
   SNMP マネージャに標準トラップを発行する設定をします。
   - コミュニティ名：NETWORK

- SNMP マネージャの IP アドレス：128.1.1.2
- 発行するトラップ：標準トラップ

21.2.5 SNMPv3 によるトラップ送信の設定

[設定のポイント]

MIB ビューと SNMP セキュリティユーザを設定の上，SNMP セキュリティグループを設定し，さらに SNMP トラップモードを設定します。

[コマンドによる設定]

1. **(config)# snmp-server view "ALL_TRAP_VIEW" * included**
   MIB ビューを設定します。
   - ビュー名 ALL_TRAP_VIEW に全サブツリーを登録します。

2. **(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789"**
   SNMP セキュリティユーザを設定します。
   - SNMP セキュリティユーザ名：ADMIN
   - SNMP セキュリティグループ名：ADMIN_GROUP
   - 認証プロトコル：HMAC-MD5
   - 認証パスワード：ABC*_1234
   - 暗号化プロトコル：CBC-DES
   - 暗号化パスワード：XYZ/+6789

3. **(config)# snmp-server group "ADMIN_GROUP" v3 priv notify "ALL_TRAP_VIEW"**
   SNMP セキュリティグループを設定します。
   - SNMP セキュリティグループ名：ADMIN_GROUP
   - セキュリティレベル：認証あり，暗号化あり
   - Notify ビュー名：ALL_TRAP_VIEW

4. **(config)# snmp-server host 128.1.1.2 traps "ADMIN" version 3 priv snmp**
   SNMPv3 によって SNMP マネージャに標準トラップを発行する設定をします。
   - SNMP マネージャの IP アドレス：128.1.1.2
   - SNMP セキュリティユーザ名：ADMIN
   - セキュリティレベル：認証あり，暗号化あり
   - 発行するトラップ：標準トラップ

21.2.6 リンクトラップの抑止

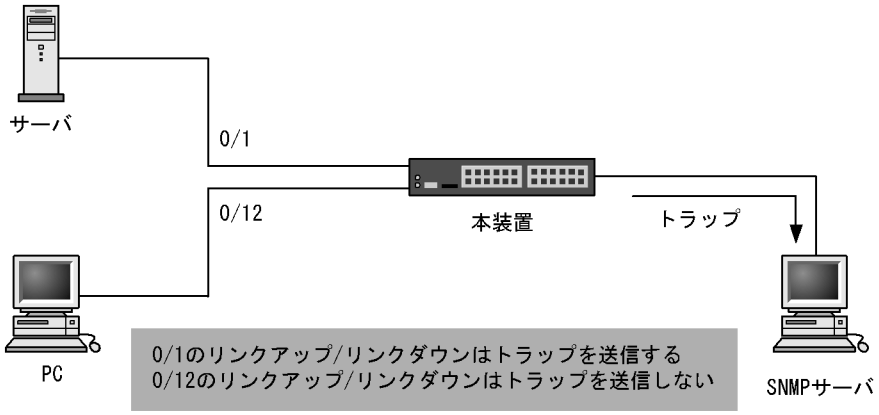
本装置は，デフォルト動作としてイーサネットインタフェースがリンクアップまたはリンクダウンしたときに，SNMP トラップを発行します。また，コンフィグレーションによって，イーサネットインタフェースごとに，リンクトラップの送信抑止を設定できます。例えば，サーバと接続する回線のように重要度の高い回線だけトラップを送信し，そのほかの回線のリンクトラップの送信を抑止することで，本装置，

ネットワーク，および SNMP マネージャの不要な処理を削減できます。

［設定のポイント］

リンクトラップの設定内容はネットワーク全体の運用方針に従って決定します。

図 21-28 リンクトラップの構成図



ここでは，ポート 0/1 については，トラップを送信するので，コンフィグレーションの設定は必要ありません。ポート 0/12 については，トラップを送信しないように設定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/12**
   (config-if)# no snmp trap link-status
   リンクアップ／リンクダウン時にトラップを送信しません。

2. **(config-if)# exit**

21.2.7 RMON イーサネットヒストリグループの制御情報の設定

［設定のポイント］

RMON（RFC1757）イーサネットの統計来歴の制御情報を設定します。本コマンドでは最大 32 エントリの設定ができます。あらかじめ SNMP マネージャを登録しておく必要があります。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/5**
   ギガビット・イーサネットインタフェース 0/5 のインタフェースモードに遷移します。

2. **(config-if)# rmon collection history controlEntry 33 owner "NET-MANAGER" buckets 10**
   統計来歴の制御情報の情報識別番号，設定者の識別情報，および統計情報を格納する来歴エントリ数を設定します。
   - 情報識別番号：33
   - 来歴情報の取得エントリ：10 エントリ
   - 設定者の識別情報：”NET-MANAGER”

21.2.8 RMON による特定 MIB 値の閾値チェック

[設定のポイント]

特定の MIB の値に対して定期的に閾値チェックを行い，閾値を超えたら SNMP マネージャにイベントを通知するように設定します。

イベント実行方法に trap を指定する場合は，あらかじめ SNMP トラップモードの設定が必要です。

[コマンドによる設定]

1. **(config)# rmon event 3 log trap public**

   アラームが発生したときに実行するイベントを設定します。
   - 情報識別番号：3
   - イベント実行方法：log，trap
   - Trap 送信コミュニティ名：public

2. **(config)# rmon alarm 12 "ifOutDiscards.3" 256111 delta rising-threshold 400000 rising-event-index 3 falling-threshold 100 falling-event-index 3 owner "NET-MANAGER"**

   RMON アラームグループの制御情報を次の条件で設定します。
   - RMON アラームグループの制御情報識別番号：12
   - 閾値チェックを行う MIB のオブジェクト識別子：ifOutDiscards.3
   - 閾値チェックを行う時間間隔：256111 秒
   - 閾値チェック方式：差分値チェック（delta）
   - 上方閾値の値：400000
   - 上方閾値を超えたときのイベント方法の識別番号：3
   - 下方閾値の値：100
   - 下方閾値を超えたときのイベント方法の識別番号：3
   - コンフィグレーション設定者の識別情報：NET-MANAGER

21.3 オペレーション

21.3.1 運用コマンド一覧

SNMP/RMON に関する運用コマンド一覧を次の表に示します。

表 21-5 運用コマンド一覧

コマンド名	説明
snmp lookup	サポート MIB オブジェクト名称およびオブジェクト ID を表示します。
snmp get	指定した MIB の値を表示します。
snmp getnext	指定した次の MIB の値を表示します。
snmp walk	指定した MIB ツリーを表示します。
snmp getif	interface グループの MIB 情報を表示します。
snmp getarp	ipNetToMediaTable（IP アドレス変換テーブル）を表示します。
snmp rget	指定したリモート装置の MIB の値を表示します。
snmp rgetnext	指定したリモート装置の次の MIB の値を表示します。
snmp rwalk	指定したリモート装置の MIB ツリーを表示します。
snmp rgetroute	指定したリモート装置の ipRouteTabler（IP ルーティングテーブル）を表示します。
snmp rgetarp	指定したリモート装置の ipNetToMediaTable（IP アドレス変換テーブル）を表示します。

21.3.2 SNMP マネージャとの通信の確認

本装置に SNMP エージェント機能を設定して SNMP プロトコルによるネットワーク管理を行う場合，次のことを確認してください。

● ネットワーク上の SNMP マネージャから本装置に対して MIB を取得できること

● 本装置からネットワーク上の SNMP マネージャへ SNMP のトラップが送信されていること

確認手順を次に示します。なお，本装置から取得できる MIB についてはマニュアル「MIB レファレンス　1. サポート MIB の概要」を，本装置から送信されるトラップについてはマニュアル「MIB レファレンス　4.2 サポートトラップ -PDU 内パラメータ」を，それぞれ参照してください。

1. ping コマンドを SNMP マネージャの IP アドレスを指定して実行し，本装置から SNMP マネージャに対して IP 通信ができることを確認してください。通信ができない場合はマニュアル「トラブルシューティングガイド」を参照してください。
2. SNMP マネージャから本装置に対して MIB の取得ができることを確認してください。取得できない場合の対応はマニュアル「トラブルシューティングガイド」を参照してください。

22 ログ出力機能

この章では，本装置のログ出力機能について説明します。

22.1 解説

本装置では動作情報や障害情報などを運用メッセージとして通知します。同メッセージは運用端末に出力するほか，運用ログとして装置内に保存します。この情報で装置の運用状態や障害の発生を管理できます。

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

- オペレータの操作および応答メッセージ
- 運用メッセージ

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

これらのログは装置内にテキスト形式で格納されています。装置管理者は，表示コマンドでこれらの情報を参照できます。

採取した本装置のログ情報は，syslog インタフェースを使用して syslog 機能を持つネットワーク上の他装置（UNIX ワークステーションなど）に送ることができます※1，※2。また，同様に，ログ情報を E-Mail を使用してネットワーク上の他装置に送ることもできます。これらのログ出力機能を使用することで，多数の装置を管理する場合にログの一元管理ができるようになります。また，ログ情報を E-Mail で送信することもできます。

注※1
他装置からの syslog メッセージを受信する機能はサポートしていません。

注※2
本装置で生成した syslog メッセージでは，RFC3164 で定義されている HEADER 部の HOSTNAME 欄は未設定です。

22.2 コンフィグレーション

22.2.1 コンフィグレーションコマンド一覧

ログ出力機能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 22-1 コンフィグレーションコマンド一覧（syslog 出力に関する設定）

コマンド名	説明
logging event-kind	syslog サーバに送信対象とするログ情報のイベント種別を設定します。
logging facility	ログ情報を syslog インタフェースで出力するためのファシリティを設定します。
logging host	ログ情報の出力先を設定します。
logging trap	syslog サーバに送信対象とするログ情報の重要度を設定します。

表 22-2 コンフィグレーションコマンド一覧（E-Mail 出力に関する設定）

コマンド名	説明
logging email	ログ情報を E-Mail で出力するための E-Mail アドレスを設定します。
logging email-event-kind	E-Mail で出力対象とするログ情報のイベント種別を設定します。
logging email-from	ログ情報を E-Mail で出力する E-Mail の送信元を設定します。
logging email-interval	ログ情報を E-Mail で出力するための送信間隔を設定します。
logging email-server	ログ情報を E-Mail で出力するため SMTP サーバの情報を設定します。

22.2.2 ログの syslog 出力の設定

[設定のポイント]

syslog 出力機能を使用して，採取したログ情報を syslog サーバに送信するための設定をします。

[コマンドによる設定]

1. **(config)# logging host LOG_HOST**
   ログをホスト名 LOG_HOST 宛てに出力するように設定します。

22.2.3 ログの E-Mail 出力の設定

[設定のポイント]

E-Mail 送信機能を使用して，採取したログ情報をリモートホスト，PC などに送信するための設定をします。

[コマンドによる設定]

1. **(config)# logging email system@loghost**
   送信先のメールアドレスとして system@loghost を設定します。

23 sFlow 統計（フロー統計）機能

この章では，本装置を中継するパケットのトラフィック特性を分析する機能である sFlow 統計の解説と操作方法について説明します。

23.1　解説

23.1.1　sFlow 統計の概要

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

図 23-1　sFlow 統計のネットワーク構成例

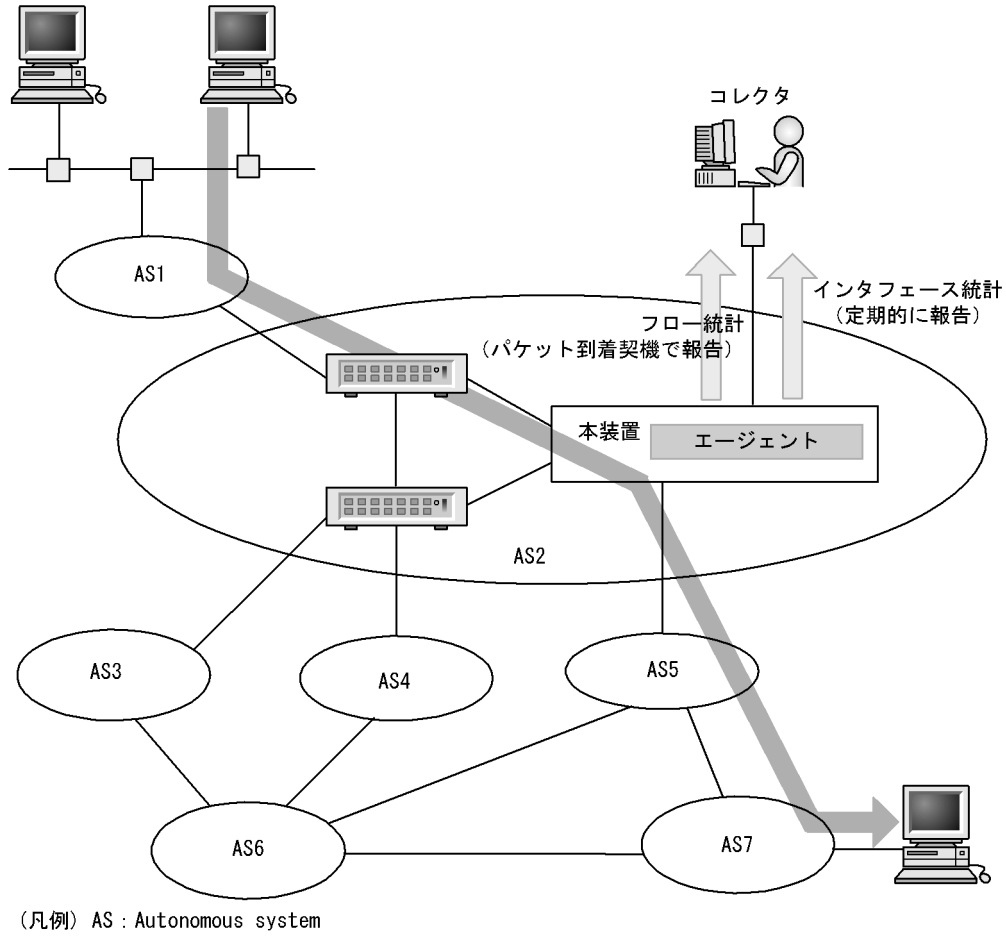
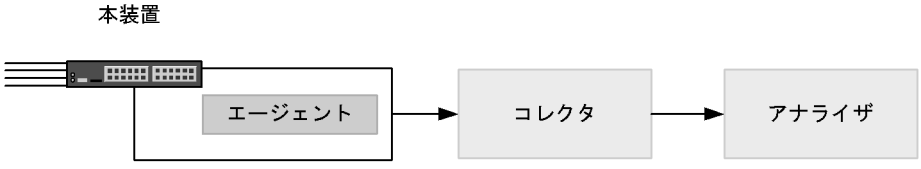


図 23-2　システム構成



本装置のエージェントでモニタされた情報はコレクタに集められ，統計結果をアナライザによってグラフィカルに表示できます。したがって，sFlow 統計機能を利用するにはコレクタとアナライザが必要です。

表 23-1　システム構成要素

構成要素	役割
エージェント（本装置）	統計情報を収集してコレクタに送付します。
コレクタ※	エージェントから送付される統計情報を集計・編集・表示します。さらに，編集データをアナライザに送付します。
アナライザ	コレクタから送付されるデータをグラフィカルに表示します。

注※　アナライザと一緒になっている場合もあります。

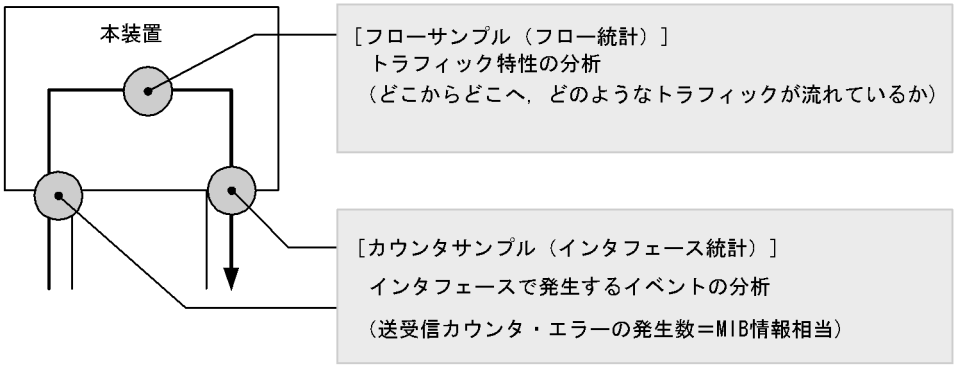
23.1.2　sFlow 統計エージェント機能

本装置のエージェントには，次の二つの機能があります。

- フロー統計（sFlow 統計ではフローサンプルと呼びます。以降，この名称で表記します。）作成機能
- インタフェース統計（sFlow 統計ではカウンタサンプルと呼びます。以降，この名称で表記します。）作成機能

フローサンプル作成機能は送受信パケット（フレーム）をユーザ指定の割合でサンプリングし，パケット情報を加工してフローサンプル形式でコレクタに送信する機能です。カウンタサンプル作成機能はインタフェース統計をカウンタサンプル形式でコレクタに送信する機能です。それぞれの収集個所と収集内容を次の図に示します。

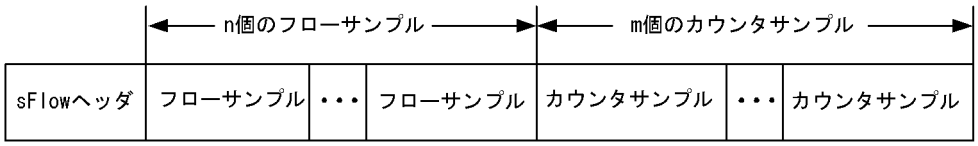
図 23-3　フローサンプルとカウンタサンプル



23.1.3　sFlow パケットフォーマット

本装置がコレクタに送信する sFlow パケット（フローサンプルとカウンタサンプル）について説明します。コレクタに送信するフォーマットは RFC3176 で規定されています。sFlow パケットのフォーマットを次の図に示します。

図 23-4 sFlow パケットフォーマット



(1) sFlow ヘッダ

sFlow ヘッダへ設定される内容を次の表に示します。

表 23-2 sFlow ヘッダのフォーマット

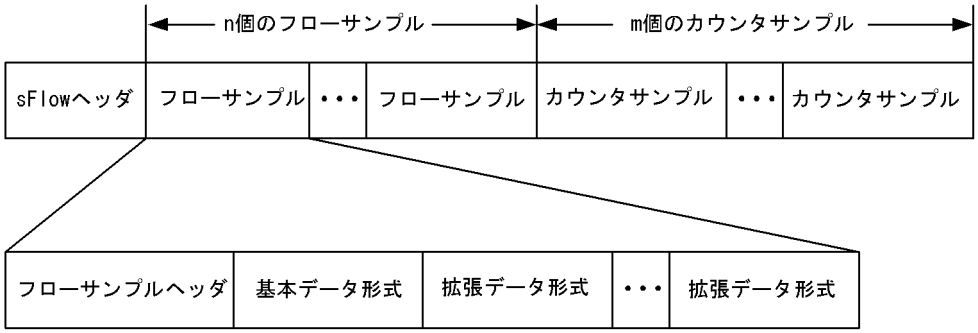
設定項目	説明	サポート
バージョン番号	sFlow パケットのバージョン（バージョン 2，4 をサポート）	○
アドレスタイプ	エージェントの IP タイプ（IPv4=1，IPv6=2）	○
エージェント IP アドレス	エージェントの IP アドレス	○
シーケンス番号	sFlow パケットの生成ごとに増加する番号	○
生成時刻	現在の時間（装置の起動時からのミリセカンド）	○
サンプル数	この信号に含まれるサンプリング（フロー・カウンタ）したパケット数 （「図 23-4 sFlow パケットフォーマット」の例では n ＋ m が設定されます）	○

（凡例）○：サポートする

(2) フローサンプル

フローサンプルとは，受信パケットのうち，他装置へ転送または本装置宛てと判定されるパケットの中から一定のサンプリング間隔でパケットを抽出し，コレクタに送信するためのフォーマットです。フローサンプルにはモニタしたパケットに加えて，パケットには含まれていない情報（受信インタフェース，送信インタフェース，AS 番号など）も収集するため，詳細なネットワーク監視ができます。フローサンプルのフォーマットを次の図に示します。

図 23-5 フローサンプルのフォーマット



(a) フローサンプルヘッダ

フローサンプルヘッダへ設定する内容を次の表に示します。

表 23-3 フローサンプルヘッダのフォーマット

設定項目	説明	サポート
sequence_number	フローサンプルの生成ごとに増加する番号	○
source_id	フローサンプルの装置内の発生源（受信インタフェース）を表す SNMP Interface Index	○
sampling_rate	フローサンプルのサンプリング間隔	○
sample_pool	インタフェースに到着したパケットの総数	○
drops	廃棄したフローサンプルの総数	○
input	受信インタフェースの SNMP Interface Index。 インタフェースが不明な場合 0 を設定	○
output	送信インタフェースの SNMP Interface Index ※。 送信インタフェースが不明な場合は 0 を設定。	×

（凡例）○：サポートする　×：サポートしない
注※　本装置では output をサポートしていないため 0 固定です。

(b) 基本データ形式

基本データ形式はヘッダ型，IPv4 型および IPv6 型の 3 種類があり，このうち一つだけ設定できます。基本データ形式のデフォルト設定はヘッダ型です。IPv4 型，IPv6 型を使用したい場合はコンフィグレーションコマンドで設定してください。各形式のフォーマットを以降の表に示します。

表 23-4 ヘッダ型のフォーマット

設定項目	説明	サポート
packet_information_type	基本データ形式のタイプ（ヘッダ型 =1）	○
header_protocol	ヘッダプロトコル番号（ETHERNET=1）	○
frame_length	オリジナルのパケット長	○
header_length	オリジナルからサンプリングした分のパケット長（デフォルト 128）	○
header<>	サンプリングしたパケットの内容	○

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

表 23-5 IPv4 型のフォーマット

設定項目	説明	サポート
packet_information_type	基本データ形式のタイプ（IPv4 型 =2）	○
length	IPv4 パケットの長さ	○
protocol	IP プロトコルタイプ（例：TCP=6，UDP=17）	○
src_ip	送信元 IP アドレス	○
dst_ip	宛先 IP アドレス	○
src_port	送信元ポート番号	○
dst_port	宛先ポート番号	○
tcp_flags	TCP フラグ	○
TOS	IP のタイプオブサービス	○

（凡例）○：サポートする

表 23-6　IPv6 型のフォーマット

設定項目	説明	サポート
packet_information_type	基本データ形式のタイプ（IPv6 型 =3）	○
length	低レイヤを除いた IPv6 パケットの長さ	○
protocol	IP プロトコルタイプ（例：TCP=6，UDP=17）	○
src_ip	送信元 IP アドレス	○
dst_ip	宛先 IP アドレス	○
src_port	送信元ポート番号	○
dst_port	宛先ポート番号	○
tcp_flags	TCP フラグ	○
priority	優先度	○

（凡例）○：サポートする

(c) 拡張データ形式

拡張データ形式はスイッチ型・ルータ型・ゲートウェイ型・ユーザ型・URL 型の 5 種類があります。拡張データ形式のデフォルト設定ではすべての拡張形式を収集し，コレクタに送信します。本形式はコンフィグレーションにより変更可能です。各形式のフォーマットを以降の表に示します。

表 23-7　拡張データ形式の種別一覧

拡張データ種別	説明	サポート
スイッチ型	スイッチ情報（VLAN 情報など）を収集する。	○
ルータ型	ルータ情報（NextHop など）を収集する。	○※1※2
ゲートウェイ型	ゲートウェイ情報（AS 番号など）を収集する。	○※1※2
ユーザ型	ユーザ情報（TACACS/RADIUS 情報など）を収集する。	○※2
URL 型	URL 情報（URL 情報など）を収集する。	○※2

（凡例）○：サポートする
注※ 1　L2 中継時は sFlow パケットに収集されません。
注※ 2　2 段以上の VLAN Tag 付きフレームが対象になった場合は，sFlow パケットに収集されません。

表 23-8　スイッチ型のフォーマット

設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（スイッチ型 =1）	○
src_vlan	受信パケットの 802.1Q VLAN ID	○
src_priority	受信パケットの 802.1p 優先度	○
dst_vlan	送信パケットの 802.1Q VLAN ID	×※
dst_priority	送信パケットの 802.1p 優先度	×※

（凡例）○：サポートする　×：サポートしない
注※　未サポートのため 0 固定です。

表 23-9 ルータ型のフォーマット

設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（ルータ型 =2）	○
nexthop_address_type	次の転送先ルータの IP アドレスタイプ	○※
nexthop	次の転送先ルータの IP アドレス	○※
src_mask	送信元アドレスのプレフィックスマスクビット	○
dst_mask	宛先アドレスのプレフィックスマスクビット	○

（凡例）○：サポートする
注※ 宛先アドレスへの経路がマルチパス経路の場合は 0 で収集されます。

表 23-10 ゲートウェイ型のフォーマット

設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（ゲートウェイ型 =3）	○
as	本装置の AS 番号	○
src_as	送信元の AS 番号	○※ 1
src_peer_as	送信元への隣接 AS 番号	○※ 1※ 2
dst_as_path_len	AS 情報数（1 固定）	○
dst_as_type	AS 経路種別（2：AS_SEQUENCE）	○
dst_as_len	AS 数（2 固定）	○
dst_peer_as	宛先への隣接 AS 番号	○※ 1
dst_as	宛先の AS 番号	○※ 1
communities<>	本経路に関するコミュニティ※ 3	×
localpref	本経路に関するローカル優先※ 3	×

（凡例）○：サポートする　×：サポートしない
注※ 1　送受信先がダイレクト経路の場合は，AS 番号が 0 で収集されます。
注※ 2　本装置から送信元を検索した場合の隣接 AS 番号です。実際に通過した隣接 AS 番号と異なる場合があります。
注※ 3　未サポートのため 0 固定です。

表 23-11 ユーザ型のフォーマット

設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（ユーザ型 =4）	○
src_user_len	送信元のユーザ名の長さ	○
src_user<>	送信元のユーザ名	○
dst_user_len	宛先のユーザ名の長さ※	×
dst_user<>	宛先のユーザ名※	×

（凡例）○：サポートする　×：サポートしない
注※ 未サポートのため 0 固定です。

表 23-12 URL 型のフォーマット

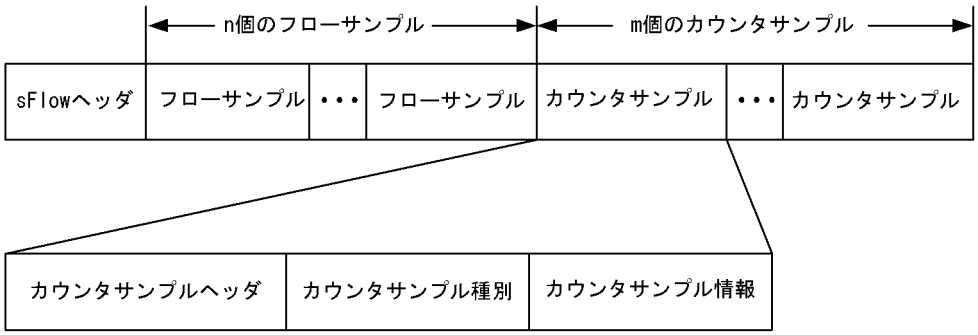
設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（URL 型 =5）	○
url_direction	URL 情報源 （source address=1，destination address=2）	○
url_len	URL 長	○
url<>	URL 内容	○

（凡例）○：サポートする

(3) カウンタサンプル

カウンタサンプルは，インタフェース統計情報（到着したパケット数や，エラーの数など）を送信します。また，インタフェースの種別よりコレクタに送信するフォーマットが決定されます。カウンタサンプルのフォーマットを次の図に示します。

図 23-6 カウンタサンプルのフォーマット



(a) カウンタサンプルヘッダ

カウンタサンプルヘッダへ設定される内容を次の表に示します。

表 23-13 カウンタサンプルヘッダのフォーマット

設定項目	説明	サポート
sequence_number	カウンタサンプルの生成ごとに増加する番号	○
source_id	カウンタサンプルの装置内の発生源（特定のポート）を表す SNMP Interface Index	○
sampling_interval	コレクタへのカウンタサンプルの送信間隔	○

（凡例）○：サポートする

(b) カウンタサンプル種別

カウンタサンプル種別はインタフェースの種別ごとに分類され収集されます。カウンタサンプル種別として設定される内容を次の表に示します。

表 23-14 カウンタサンプル種別一覧

設定項目	説明	サポート
GENERIC	一般的な統計（counters_type=1）	×※1

設定項目	説明	サポート
ETHERNET	イーサネット統計（counters_type=2）	○
TOKENRING	トークンリング統計（counters_type=3）	×※1
FDDI	FDDI 統計（counters_type=4）	×※1
100BaseVG	VG 統計（counters_type=5）	×※1
WAN	WAN 統計（counters_type=6）	×※1
VLAN	VLAN 統計（counters_type=7）	×※2

（凡例）○：サポートする　×：サポートしない
注※1　本装置で未サポートなインタフェースタイプのためです。
注※2　本装置では VLAN 統計はサポートしていません。

(c) カウンタサンプル情報

カウンタサンプル情報はカウンタサンプル種別により収集される内容が変わります。VLAN 統計以外は MIB で使われている統計情報（RFC）に従って送信されます。カウンタサンプル情報として設定される内容を次の表に示します。

表 23-15　カウンタサンプル情報

設定項目	説明	サポート
GENERIC	一般的な統計［RFC2233 参照］	×
ETHERNET	イーサネット統計［RFC2358 参照］	○※
TOKENRING	トークンリング統計［RFC1748 参照］	×
FDDI	FDDI 統計［RFC1512 参照］	×
100BaseVG	VG 統計［RFC2020 参照］	×
WAN	WAN 統計［RFC2233 参照］	×
VLAN	VLAN 統計［RFC3176 参照］	×

（凡例）○：サポートする　×：サポートしない
注※　イーサネット統計のうち ifDirection，dot3StatsSymbolErrors，ifOutUcastPkts は収集できません。

23.1.4　本装置での sFlow 統計の動作について

(1) sFlow 統計収集の対象パケットに関する注意点

- 本装置での sFlow 統計は，受信パケットと送信パケットを対象パケットとして扱います。
- 送信時に廃棄と判定されるパケット（フィルタ機能で廃棄判定されるパケットなど）は，sFlow 統計収集の対象外パケットとして扱います。
- ソフトウェア中継パケットや自発パケット，自宛パケットは sFlow 統計収集の対象外パケットとして扱います。
- ポートミラーリングのミラーポートからの送信パケットは，sFlow 統計収集の対象外パケットとして扱います。

(2) データ収集位置による注意点

- ingress 指定および egress 指定のどちらで検出されても，sFlow パケットの内容は本装置に入ってきた時点のパケット内容が収集されます（本装置内でパケット内容の変換などが行われても，sFlow パケットには反映されません。）。

- 本装置での sFlow 統計は，受信パケットまたは送信パケットをサンプリングしてコレクタに送信します。この性質上，受信側にフィルタ機能や QoS 機能を設定してパケットを廃棄する条件でも，コレクタには中継しているように送信する場合があります。フィルタ機能や QoS 機能と併用するときは，パケットが廃棄される条件をご確認の上運用してください。他機能と併用時の sFlow 統計収集条件を次の表に示します。

表 23-16　他機能と併用時の sFlow 統計収集条件

機能	受信パケットが sFlow 統計対象	送信パケットが sFlow 統計対象
フィルタ機能	廃棄対象でも収集される	廃棄対象は収集されない※
QoS 機能（受信側）	廃棄対象でも収集される	廃棄対象は収集されない※
QoS 機能（送信側）	廃棄対象でも収集される	廃棄対象でも収集される※
自宛	収集されない	収集されない
自発	収集されない	収集されない

注※　sFlow パケットの内容は，本装置に入ってきた時点のパケット内容が収集されます。

23.2 コンフィグレーション

23.2.1 コンフィグレーションコマンド一覧

sFlow 統計で使用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 23-17 コンフィグレーションコマンド一覧

コマンド名	説明
sflow destination	sFlow パケットの宛先であるコレクタの IP アドレスを指定します。
sflow extended-information-type	フローサンプルの各拡張データ形式の送信有無を指定します。
sflow forward egress	指定したポートの送信トラフィックを sFlow 統計の監視対象にします。
sflow forward ingress	指定したポートの受信トラフィックを sFlow 統計の監視対象にします。
sflow max-header-size	基本データ形式（sflow packet-information-type コマンド参照）にヘッダ型を使用している場合，サンプルパケットの先頭からコピーされる最大サイズを指定します。
sflow max-packet-size	sFlow パケットのサイズを指定します。
sflow packet-information-type	フローサンプルの基本データ形式を指定します。
sflow polling-interval	カウンタサンプルをコレクタへ送信する間隔を指定します。
sflow sample	装置全体に適用するサンプリング間隔を指定します。
sflow source	sFlow パケットの送信元（エージェント）に設定される IP アドレスを指定します。
sflow url-port-add	拡張データ形式で URL 情報を使用する場合に，HTTP パケットと判断するポート番号を 80 以外に追加指定します。
sflow version	送信する sFlow パケットのバージョンを設定します。

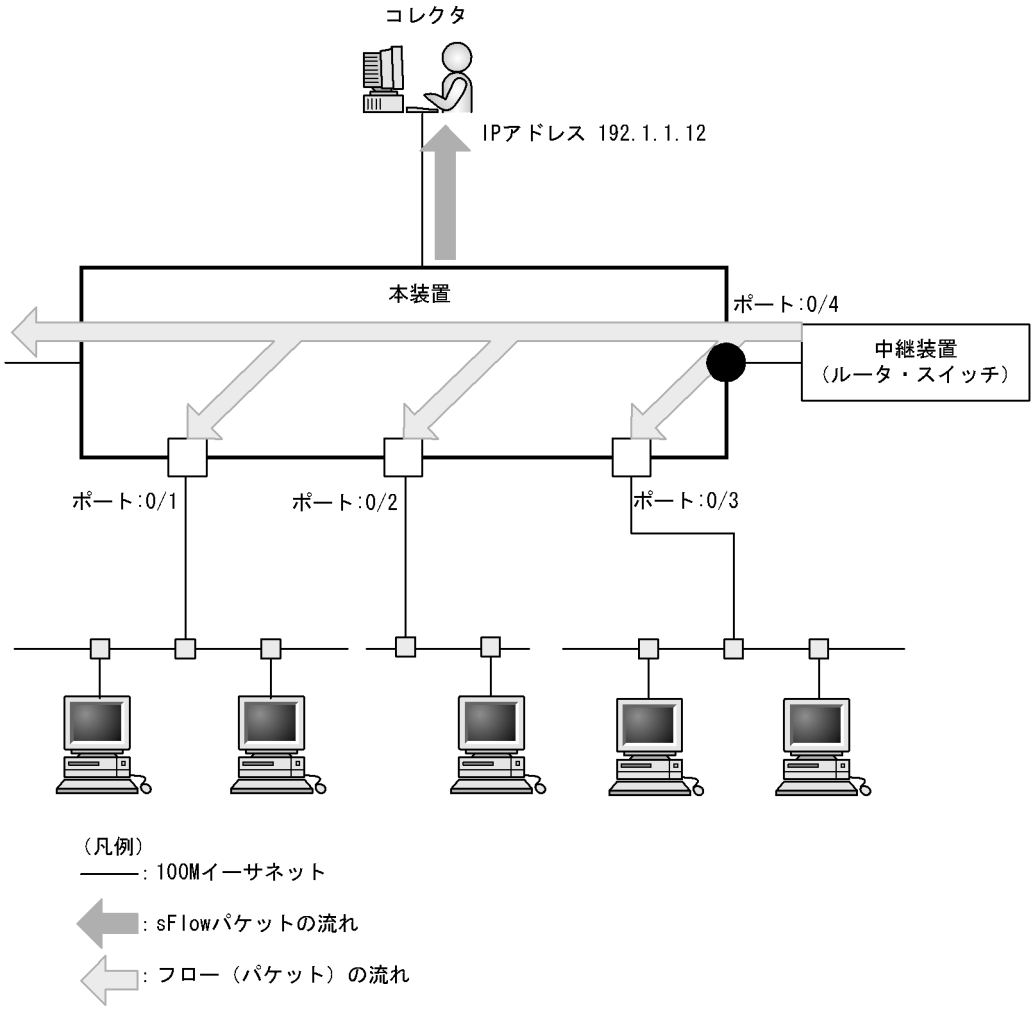
23.2.2 sFlow 統計の基本的な設定

(1) 受信パケットをモニタする設定

[設定のポイント]

sFlow 統計のコンフィグレーションは装置全体で有効な設定と，実際に運用するポートを指定する設定の二つが必要です。ここではポート 0/4 に対して入ってくるパケットをモニタする設定を示します。

図 23-7　ポート 0/4 の受信パケットをモニタする設定例



[コマンドによる設定]

1. **(config)# sflow destination 192.1.1.12**
   コレクタとして IP アドレス 192.1.1.12 を設定します。

2. **(config)# sflow sample 512**
   512 パケットごとにトラフィックをモニタします。

3. **(config)# interface gigabitethernet 0/4**
   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

4. **(config-if)# sflow forward ingress**
   ポート 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

[注意事項]

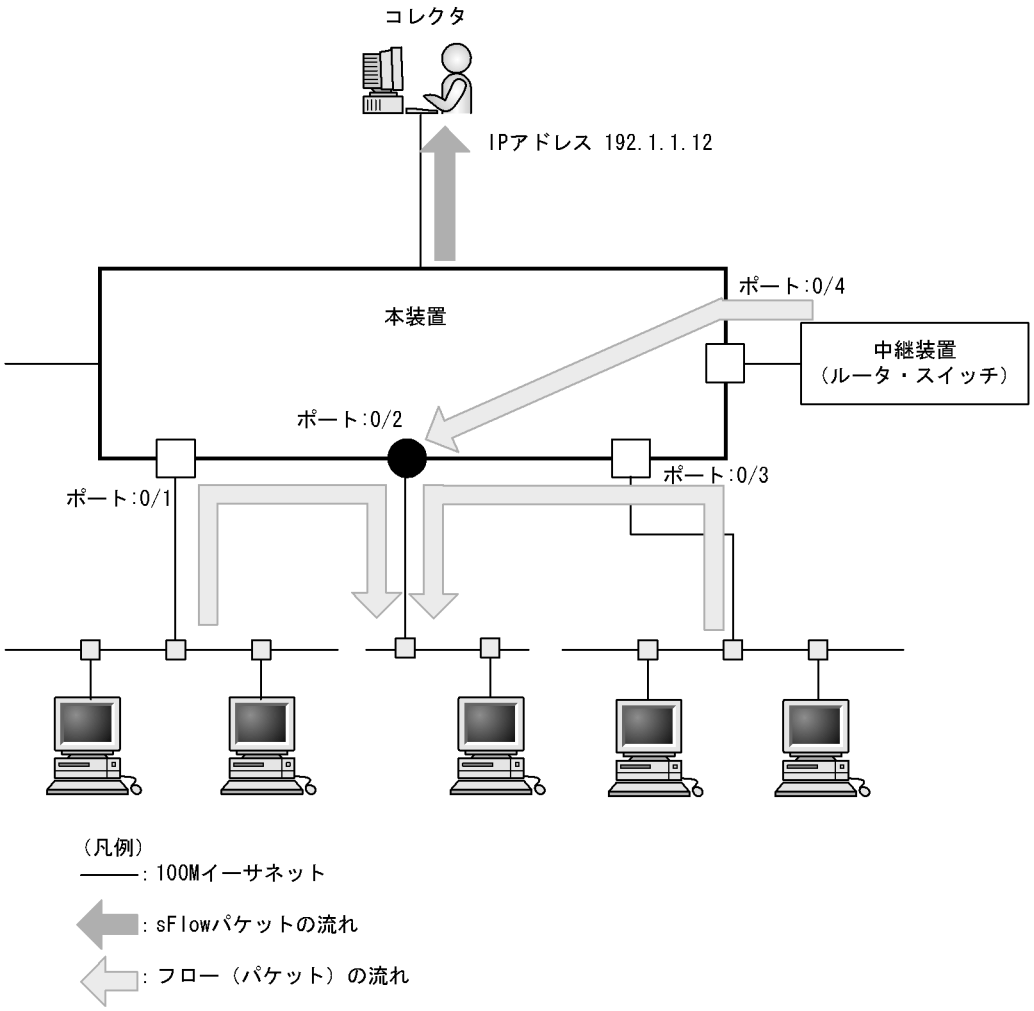
sflow sample コマンドで設定するサンプリング間隔については，インタフェースの回線速度を考慮して決める必要があります。詳細は，「コンフィグレーションコマンドレファレンス　sflow sample」を参照してください。

(2) 送信パケットをモニタする設定

[設定のポイント]

sFlow 統計機能を，受信パケットまたは送信パケットのどちらに対して有効にするかは，インタフェースコンフィグレーションモードで設定するときに sflow forward ingress コマンドまたは sflow forward egress コマンドのどちらを指定するかによって決まります。ここではポート 0/2 から出て行くパケットをモニタする設定を示します。

図 23-8 ポート 0/2 の送信パケットをモニタする設定例



[コマンドによる設定]

1. **(config)# sflow destination 192.1.1.12**
   コレクタとして IP アドレス 192.1.1.12 を設定します。

2. **(config)# sflow sample 512**
   512 パケットごとにトラフィックをモニタします。

3. **(config)# interface gigabitethernet 0/2**
   ポート 0/2 のイーサネットインタフェースコンフィグレーションモードに移行します。

4. **(config-if)# sflow forward egress**
   ポート 0/2 の送信パケットに対して sFlow 統計機能を有効にします。

[注意事項]

1. 次のモデルでは本設定はできません。
   ・AX2430S-48T，AX2430S-48TD および AX2430S-48T2X

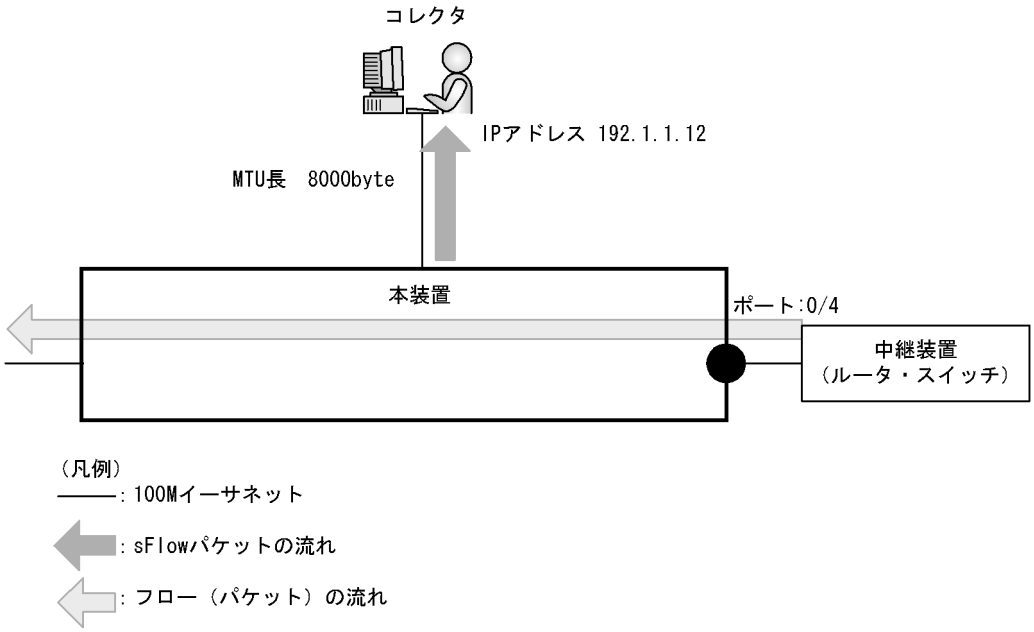
23.2.3 sFlow 統計コンフィグレーションパラメータの設定例

（1） MTU 長と sFlow パケットサイズの調整

[設定のポイント]

sFlow パケットはデフォルトでは 1400byte 以下のサイズでコレクタに送信されます。コレクタへの回線の MTU 値が大きい場合，同じ値に調整することでコレクタに対して効率よく送信できます。ここでは MTU 長が 8000byte の回線とコレクタが繋がっている設定を記述します。

図 23-9 コレクタへの送信を MTU=8000byte に設定する例



[コマンドによる設定]

1. **(config)# sflow destination 192.1.1.12**
   コレクタとして IP アドレス 192.1.1.12 を設定します。

2. **(config)# sflow sample 32**
   32 パケットごとにトラフィックをモニタします。

3. **(config)# sflow max-packet-size 8000**
   sflow パケットサイズの最大値を 8000byte に設定します。

4. **(config)# interface gigabitethernet 0/4**
   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

5. **(config-if)# sflow forward ingress**
   ポート 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

(2) 収集したい情報を絞る

[設定のポイント]

sFlow パケットの情報はコンフィグレーションを指定しないとすべて収集する条件になっています。しかし，不要な情報がある場合に，その情報を取らない設定をすることで CPU 使用率を下げることができます。ここでは IP アドレス情報だけが必要な場合の設定を記述します。

[コマンドによる設定]

1. **(config)# sflow destination 192.1.1.12**
   コレクタとして IP アドレス 192.1.1.12 を設定します。

2. **(config)# sflow sample 512**
   512 パケットごとにトラフィックをモニタします。

3. **(config)# sflow packet-information-type ip**
   フローサンプルの基本データ形式に IP 形式を設定します。

4. **(config)# sflow extended-information-type router**
   フローサンプルの拡張データ形式に「ルータ」を設定します（ルータ情報だけが取得できます）。

5. **(config)# interface gigabitethernet 0/4**
   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

6. **(config-if)# sflow forward ingress**
   ポート 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

(3) sFlow パケットのエージェント IP アドレスを固定化する

[設定のポイント]

一般的なコレクタは，sFlow パケットに含まれるエージェント IP アドレスの値を基にして同一の装置かどうかを判断しています。この理由から，sflow source コマンドや interface loopback コマンドでエージェント IP アドレスを設定していない場合，コレクタ側で複数装置から届いているように表示されるおそれがあります。長期的に情報を見る場合はエージェント IP アドレスを固定化してください。ここでは loopback に割り当てられた IP アドレスをエージェント IP アドレスとして利用し，コレクタに送る設定を示します。

[コマンドによる設定]

1. **(config)# interface loopback 0**
   ループバックインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# ip address 176.1.1.11**
   ループバックインタフェースに IPv4 用として 176.1.1.11 を設定します。

3. **(config-if)# ipv6 address 3ffe:100::1**
   (config-if)# exit
   ループバックインタフェースに IPv6 用として 3ffe:100::1 を設定します。

4. **(config)# sflow destination 192.1.1.12**
   コレクタとして IP アドレス 192.1.1.12 を設定します。

5. **(config)# sflow sample 512**
   512 パケットごとにトラフィックをモニタします。

6. **(config)# interface gigabitethernet 0/4**
   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

7. **(config-if)# sflow forward ingress**
   ポート 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

[注意事項]

loopback の IP アドレスを使う場合は，sflow source コマンドで設定する必要はありません。もし，sflow source コマンドで IP アドレスが指定されているとその IP アドレスが優先されます。

(4) ローカルネットワーク環境での URL 情報収集

[設定のポイント]

本装置では sFlow 統計で URL 情報（HTTP パケット）を収集する場合，宛先のポート番号として 80 番を利用している環境がデフォルトになっています。しかし，ローカルなネットワークではポート番号が異なる場合があります。ローカルネットワーク環境で HTTP パケットのポート番号として 8080 番を利用している場合の設定を示します。

[コマンドによる設定]

1. **(config)# sflow destination 192.1.1.12**
   コレクタとして IP アドレス 192.1.1.12 を設定します。

2. **(config)# sflow sample 512**
   512 パケットごとにトラフィックをモニタします。

3. **(config)# sflow url-port-add 8080**
   拡張データ形式で URL 情報を使用する場合に，HTTP パケットと判断する宛先ポート番号 8080 を追加で設定します。

4. **(config)# interface gigabitethernet 0/4**
   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

5. **(config-if)# sflow forward ingress**
   ポート 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

[注意事項]

本パラメータを設定した後でも，HTTP パケットの対象として宛先ポート番号 80 番は有効です。

23.3 オペレーション

23.3.1 運用コマンド一覧

sFlow 統計で使用する運用コマンド一覧を次の表に示します。

表 23-18 運用コマンド一覧

コマンド名	説明
show sflow	sFlow 統計機能についての設定条件と動作状況を表示します。
clear sflow statistics	sFlow 統計で管理している統計情報をクリアします。
restart sflow	フロー統計プログラムを再起動します。
dump sflow	フロー統計プログラム内で収集しているデバック情報をファイル出力します。

23.3.2 コレクタとの通信の確認

本装置で sFlow 統計機能を設定してコレクタに送信する場合，次のことを確認してください。

(1) コレクタとの疎通確認

ping コマンドをコレクタの IP アドレスを指定して実行し，本装置からコレクタに対して IP 通信ができることを確認してください。通信ができない場合は，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。

(2) sFlow パケット通信確認

コレクタ側で sFlow パケットを受信していることを確認してください。

受信していない場合の対応は，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。

23.3.3 sFlow 統計機能の運用中の確認

本装置で sFlow 統計機能を使用した場合，運用中の確認内容には次のものがあります。

(1) sFlow パケット廃棄数の確認

show sflow コマンドを実行して sFlow 統計情報を表示し，sFlow 統計機能で Dropped sFlow samples（廃棄しているパケット数）や Overflow Time of sFlow Queue（廃棄パケット時間）を確認してください。どちらかの値が増加する場合は，増加しないサンプリング間隔を設定してください。

図 23-10 show sflow コマンドの実行結果

```
> show sflow
Date 2006/12/13 14:10:32 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared:  16:00:05
sFlow agent data :
  sFlow service version : 4
  CounterSample interval rate: 60 seconds
  Default configured rate: 1 per 2048 packets
  Default actual rate    : 1 per 2048 packets
  Configured sFlow ingress ports :  0/2-4
  Configured sFlow egress ports  :  ----
  Received sFlow samples : 37269  Dropped sFlow samples         :    2093
  Exported sFlow samples : 37269  Couldn't export sFlow samples :       0
  Overflow time of sFlow queue: 12 seconds                                  …1
sFlow collector data :
  Collector IP address: 192.168.4.199  UDP:6343  Source IP address: 130.130.130.1
   Send FlowSample UDP packets    : 12077  Send failed packets:     0
   Send CounterSample UDP packets:   621  Send failed packets:     0
  Collector IP address: 192.168.4.203  UDP:65535  Source IP address: 130.130.130.1
   Send FlowSample UDP packets    : 12077  Send failed packets:     0
   Send CounterSample UDP packets:   621  Send failed packets:     0
```

1. 廃棄パケット時間が増加している場合，サンプリング間隔の設定を見直してください。

（2） CPU 使用率の確認

show cpu コマンドを実行して CPU 使用率を表示し，負荷を確認してください。CPU 使用率が高い場合は，コンフィグレーションコマンド sflow sample でサンプリング間隔を再設定してください。

図 23-11 show cpu コマンドの実行結果

```
>show cpu minutes
Date 2006/12/13 14:15:37 UTC
*** minute ***
date    time              cpu average
Dec 13  14:42:00-14:42:59     6
Dec 13  14:43:00-14:43:59    20
                     :
                     :
Dec 13  15:41:00-15:41:59    10                 …1
```

1. CPU 使用率が高くなっている場合，サンプリング間隔の設定を見直してください。

23.3.4 sFlow 統計のサンプリング間隔の調整方法

本装置で sFlow 統計機能を使用した場合，サンプリング間隔の調整方法として次のものがあります。

（1） 回線速度から調整する

sFlow 統計機能を有効にしている全ポートの pps を show interfaces コマンドで確認し，受信パケットを対象にしている場合は「Input rate」を合計してください。もし，送信パケットを対象にしている場合は，「Output rate」も合計してください。その合計値を 100 で割った値が，目安となるサンプリング間隔となります。この値でサンプリング間隔を設定後，show sflow コマンドで廃棄数が増えないかどうかを確認してください。

ポート 0/4 とポート 0/5 に対して受信パケットをとる場合の目安となるサンプリング間隔の例を次に示します。

図 23-12 show interfaces コマンドの実行結果

```
> show interfaces gigabitethernet 0/4
Date 2006/12/24 17:18:54 UTC
NIF0:
Port4: active up  100BASE-TX full(auto)    0012.e220.ec30
        Time-since-last-status-change:1:47:47
        Bandwidth:10000kbps  Average out:0Mbps  Average in:5Mbps
        Peak out:5Mbps at 15:44:36  Peak in:5Mbps at 15:44:18
        Output rate:       0.0bps         0.0pps
        Input  rate:    4063.5kbps       10.3kpps
        Flow control send   :off
        Flow control receive:off
        TPID:8100
                              :

> show interfaces gigabitethernet 0/5
Date 2006/12/24 17:19:34 UTC
NIF0:
Port5: active up  100BASE-TX full(auto)    0012.e220.ec31
        Time-since-last-status-change:1:47:47
        Bandwidth:10000kbps  Average out:5Mbps  Average in:5Mbps
        Peak out:5Mbps at 15:44:36  Peak in:5Mbps at 15:44:18
        Output rate:    4893.5kbps       16.8kpps
        Input  rate:    4893.5kbps       16.8kpps
        Flow control send   :off
        Flow control receive:off
        TPID:8100
                              :
```

目安となるサンプリング間隔

＝ sFlow 統計機能を有効にしているポートの PPS 合計値 /100

＝ （10.3kpps+16.8kpps）/100

＝ 271※

注※ サンプリング間隔を 271 で設定すると実際は 512 で動作します。サンプリング間隔の詳細はコンフィグレーションコマンド sflow sample を参照してください。

（2） 詳細情報から調整する

show sflow detail コマンドを実行して表示される Sampling rate to collector（廃棄が発生しない推奨するサンプリング間隔）の値をサンプリング間隔として設定します。設定後は clear sflow statistics コマンドを実行し，しばらく様子を見てまだ Sampling rate to collector の値が設定より大きい場合は同じ手順でサンプリング間隔を設定してください。

図 23-13 show sflow detail コマンドの実行結果

```
> show sflow detail
Date 2006/12/21 20:04:01 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared:  8:00:05
                              :
   Collector IP address: 192.168.4.203  UDP:65535  Source IP address:
130.130.130.1
   Send FlowSample UDP packets   : 12077  Send failed packets:     0
   Send CounterSample UDP packets:   621  Send failed packets:     0
Detail data :
   Max packet size: 1400 bytes
   Packet information type: header
   Max header size: 128 bytes
   Extended information type: switch,router,gateway,user,url
   Url port number: 80,8080
   Sampling mode: random-number
   Sampling rate to collector: 1 per 2163 packets
   Target ports for CounterSample: 0/2-4
```

24 LLDP

この章では，本装置に隣接する装置の情報を収集する機能である LLDP の解説と操作方法について説明します。

24.1 解説

24.1.1 概要

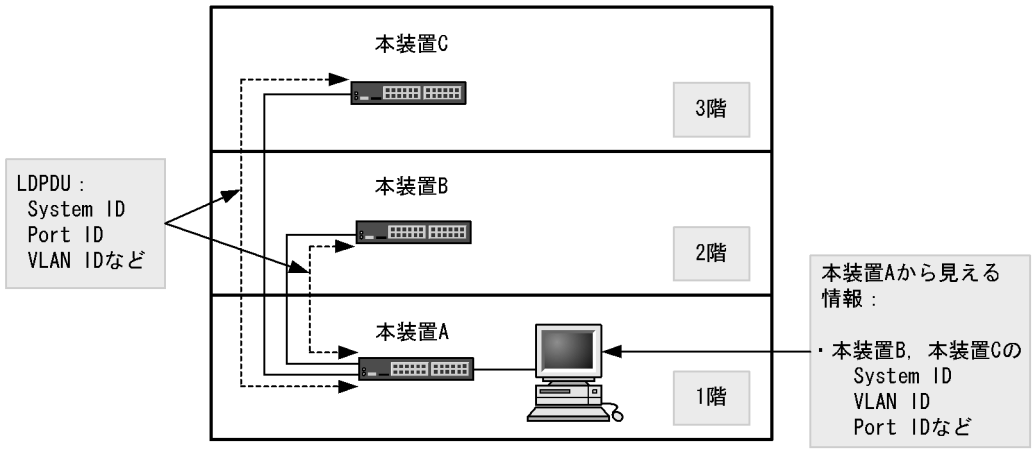
LLDP（Link Layer Discovery Protocol）は隣接する装置情報を収集するプロトコルです。運用・保守時に接続装置の情報を簡単に調査できることを目的とした機能です。

(1) LLDP の適用例

LLDP 機能を使用することで隣接装置と接続している各ポートに対して，自装置に関する情報および該当ポートに関する情報を送信します。該当ポートで受信した隣接装置の情報を管理することで自装置と隣接装置間の接続状態を把握できるようになります。

LLDP の適用例を次の図に示します。この例では，同一ビル内の各階に設置された本装置間の接続状態を，1 階に設置した本装置 A から把握できるようになります。

図 24-1 LLDP の適用例



24.1.2 サポート仕様

この機能を用いて隣接装置に配布する情報は，IEEE 802.1AB Draft 6 をベースに拡張機能として本装置独自の情報をサポートしています。サポートする情報を次の表に示します。

表 24-1 LLDP でサポートする情報

項番		名称	説明
1		Time-to-Live	情報の保持時間
2		Chassis ID	装置の識別子
3		Port ID	ポート識別子
4		Port description	ポート種別
5		System name	装置名称
6		System description	装置種別
7	—	Organizationally-defined TLV extensions	ベンダー・組織が独自に定めた TLV
	a	VLAN ID	設定されている VLAN ID
	b	VLAN Address	VLAN に関連づけられた IP アドレス

（凡例） －：該当なし

LLDP でサポートする情報の詳細を以下に示します。

なお，MIB についてはマニュアル「MIB レファレンス」を参照してください。

（1） Time-to-Live（情報の保持時間）

配布する情報を受信装置側で保持する時間を示します。

保持時間はコンフィグレーションで変更できますが，初期状態で使用することをお勧めします。

（2） Chassis ID（装置の識別子）

装置を識別する情報です。この情報には subtype が定義され，subtype によって送信内容が異なります。subtype と送信内容を次の表に示します。

表 24-2　Chassis ID の subtype 一覧

subtype	種別	送信内容
1	Chassis component	Entity MIB の entPhysicalAlias と同じ値
2	Chassis interface	interface MIB の ifAlias と同じ値
3	Port	Entity MIB の portEntPhysicalAlias と同じ値
4	Backplane component	Entity MIB の backplaneEntPhysicalAlias と同じ値
5	MAC address	LLDP MIB の macAddress と同じ値
6	Network address	LLDP MIB の networkAddress と同じ値
7	Locally assigned	LLDP MIB の local と同じ値

Chassis ID についての送受信条件は次のとおりです。

- 送信：subtype ＝ 5 だけ送信します。送信する MAC アドレスは装置 MAC アドレスを使用します。
- 受信：上記に示した全 subtype について受信できます。
- 受信データ最大長：255byte

（3） Port ID（ポート識別子）

ポートを識別する情報です。この情報には subtype が定義され，subtype によって送信内容が異なります。subtype と送信内容を次の表に示します。

表 24-3　Port ID の subtype 一覧

subtype	種別	送信内容
1	Port	Interface MIB の ifAlias と同じ値
2	Port component	Entity MIB の portEntPhysicalAlias と同じ値
3	Backplane component	Entity MIB の backplaneEntPhysicalAlias と同じ値
4	MAC address	LLDP MIB の macAddr と同じ値
5	Network address	LLDP MIB の networkAddr と同じ値
6	Locally assigned	LLDP MIB の local と同じ値

Port ID についての送受信条件は次のとおりです。

- 送信：subtype ＝ 4 だけ送信します。送信する MAC アドレスは該当 Port の MAC アドレスを使用します。
- 受信：上記に示した全 subtype について受信できます。
- 受信データ最大長：255Byte

（4） Port description（ポート種別）

ポートの種別を示す情報です。この情報には subtype はありません。

送信内容および受信条件は次のとおりです。

- 送信内容：「Interface MIB の ifDescr と同じ値」
- 受信データ最大長：255Byte

（5） System name（装置名称）

装置名称を示す情報です。この情報には subtype はありません。

送信内容および受信条件は次のとおりです。

- 送信内容：「systemMIB の sysName と同じ値」
- 受信データ最大長：255Byte

（6） System description（装置種別）

装置の種別を示す情報です。この情報には subtype はありません。

送信内容および受信条件は次のとおりです。

- 送信内容：「systemMIB の sysDescr と同じ値」
- 受信データ最大長：255Byte

（7） Organizationally-defined TLV extensions

本装置独自に以下の情報をサポートしています。

(a) VLAN ID

該当ポートが使用する VLAN Tag の VLAN ID を示します。Tag 変換機能を使用している場合は，変換後の VLAN ID を示します。この情報はトランクポートだけ有効な情報です。

(b) VLAN Address

この情報は，IP アドレスが設定されている VLAN があれば，その VLAN ID とその IP アドレスを一つ示します。

24.1.3 LLDP 使用時の注意事項

（1） 本機能を設定した装置間に本機能をサポートしない別装置を接続した場合

次に示す構成とした場合，隣接装置との接続状態を正確に把握しにくい状態になります。

- スイッチを経由して接続した場合，スイッチは LLDP の配布情報を中継します。そのため，直接接続していない装置間で，隣接情報として配布情報を受信できるので，直接接続されている装置間の情報と区別が付かなくなります。
- ルータを経由して接続した場合，LLDP の配布情報はルータで廃棄されるため LLDP 機能を設定した

装置間では受信できません。

(2) 他社接続について

他社が独自にサポートしている Link Layer Discovery Protocol※との相互接続はできません。

注※

Cisco Systems 社：CDP（Cisco Discovery Protocol）
Extreme Networks 社：EDP（Extreme Discovery Protocol）
Foundry Networks 社：FDP（Foundry Discovery Protocol）

(3) IEEE 802.1AB 規格との接続について

本装置の LLDP は IEEE 802.1AB Draft 6 をベースにサポートした独自機能です。IEEE 802.1AB 規格との接続性はありません。

(4) 隣接装置の最大数について

装置当たり最大 50 の隣接装置情報を収容できます。最大数を超えた場合，受信した配布情報は廃棄します。受信済みの隣接装置情報がタイムアウトで削除される時間を確保するために，廃棄状態は一定時間継続されます。時間は，最大収容数の閾値以上になった隣接装置情報の保持時間と同一です。

(5) CFM との共存について

CFM とは同時に使用できません。

24.2 コンフィグレーション

24.2.1 コンフィグレーションコマンド一覧

LLDP のコンフィグレーションコマンド一覧を次の表に示します。

表 24-4 コンフィグレーションコマンド一覧

コマンド名	説明
lldp enable	ポートで LLDP の運用を開始します。
lldp hold-count	本装置が送信する LLDP フレームに対して隣接装置が保持する時間を指定します。
lldp interval-time	本装置が送信する LLDP フレームの送信間隔を指定します。
lldp run	装置全体で LLDP 機能を有効にします。

24.2.2 LLDP の設定

(1) LLDP 機能の設定

[設定のポイント]

LLDP 機能のコンフィグレーションは装置全体で機能を有効にする設定と，実際に運用するポートで有効にする設定が必要です。

ここでは，gigabitethernet 0/1 において LLDP 機能を運用させます。

[コマンドによる設定]

1. **(config)# lldp run**
   装置全体で LLDP 機能を有効にします。

2. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。

3. **(config-if)# lldp enable**
   ポート 0/1 で LLDP 機能の動作を開始します。

(2) LLDP フレームの送信間隔，保持時間の設定

[設定のポイント]

LLDP フレームの送信間隔を変更すると，装置の情報の変更が反映される時間を調整できます。送信間隔を短くすると変更が早く反映され，送信間隔を長くすると変更の反映が遅くなります。

[コマンドによる設定]

1. **(config)# lldp interval-time 60**
   LLDP フレームの送信間隔を 60 秒に設定します。

2. **(config)# lldp hold-count 3**
   本装置が送信した情報を隣接装置が保持する時間を interval-time 時間の回数で設定します。この場合，60 秒× 3 で 180 秒になります。

24.3 オペレーション

24.3.1 運用コマンド一覧

LLDP の運用コマンド一覧を次の表に示します。

表 24-5 運用コマンド一覧

コマンド名	説明
show lldp	LLDP の設定情報および隣接装置情報を表示します。
show lldp statistics	LLDP の統計情報を表示します。
clear lldp	LLDP の隣接情報をクリアします。
clear lldp statistics	LLDP の統計情報をクリアします。
restart lldp	LLDP プログラムを再起動します。
dump protocols lldp	LLDP プログラムで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

24.3.2 LLDP 情報の表示

LLDP 情報の表示は，運用コマンド show lldp で行います。show lldp コマンドは，LLDP の設定情報とポートごとの隣接装置数を表示します。show lldp detail コマンドは，隣接装置の詳細な情報を表示します。

図 24-2 show lldp コマンドの実行結果

```
> show lldp
Date 2005/11/09 19:16:20 UTC
Status: Enabled Chassis ID: Type=MAC      Info=0012.e268.2c21
Interval Time: 30   Hold Count: 4  TTL:120
Port Counts=3
0/1 (CH:10)  Link:Up    Neighbor Counts:  2
0/2          Link:Down  Neighbor Counts:  0
0/3          Link:Up    Neighbor Counts:  0
>
```

図 24-3 show lldp detail コマンドの実行結果

```
> show lldp detail
Date 2005/11/09 19:16:34 UTC
Status: Enabled  Chassis ID: Type= MAC    Info=0012.e268.2c21
Interval Time: 30  Hold Count: 4  TTL:120
System Name: LLDP1
System Description: ALAXALA AX2430S AX-2430S-48T [AX2430S-48T] Switching software
Ver. 10.0 [OS-L2]
Total Neighbor Counts=2
Port Counts=3
Port 0/1 (CH:10)  Link: Up   Neighbor Counts:   2
  Port ID: Type=MAC     Info=0012.e298.5cc0
  Port Description: GigabitEther 0/1
  Tag ID: Tagged=1,10-20,4094
  IPv4 Address: Tagged: 10    192.168.248.240
  1  TTL:110    Chassis ID: Type=MAC       Info=0012.e268.2505
     System Name: LLDP2
     System Description: ALAXALA AX2430S AX-2430S-48T [AX2430S-48T] Switching
```

```
software Ver. 10.0 [OS-L2]
     Port ID: Type=MAC       Info=0012.e298.dc20
     Port Description: GigabitEther 0/5
     Tag ID: Tagged=1,10-20,4094
     IPv4 Address: Tagged: 10    192.168.248.220
  2  TTL:100    Chassis ID: Type=MAC       Info=0012.e268.2c2d
     System Name: LLDP3
    System Description: ALAXALA AX3630S AX-3630S-24T2X [AX3630S-24T2X] Switching
software Ver. 10.0 [OS-L3L]
     Port ID: Type=MAC       Info=0012.e298.7478
     Port Description: GigabitEther 0/24
     Tag ID: Tagged=1,10-20,4094
     IPv4 Address: Tagged: 10    192.168.248.200
     IPv6 Address: Tagged: 20    3ffe:501:811:ff01:200:8798:7478:e7f4
Port 0/2          Link: Down  Neighbor Counts:  0
Port 0/3          Link: Up    Neighbor Counts:  0
>
```

25 OADP

この章では，本装置に隣接する装置の情報を収集する機能である OADP の解説と操作方法について説明します。

25.1 解説

25.1.1 概要

(1) OADP 機能の概要

OADP（Octpower Auto Discovery Protocol）機能とは，本装置のレイヤ 2 レベルで動作する機能で，OADP PDU（Protocol Data Unit）のやりとりによって隣接装置の情報を収集し，隣接装置の接続状況を表示できます。

この機能では，隣接装置の装置情報やポート情報を表示することで隣接装置との接続状況を容易に把握できることから，隣接装置にログインしたりネットワーク構成図を参照したりしなくても，装置間の接続の状況を確認できます。また，この機能によって表示される接続状況とネットワーク構成図を比較することで，装置間が正しく接続されているかどうかを確認できます。

隣接装置として認識できる装置には，本装置のほかに，CDP を実装した装置，OADP を実装した装置があります。

(2) CDP 受信機能の概要

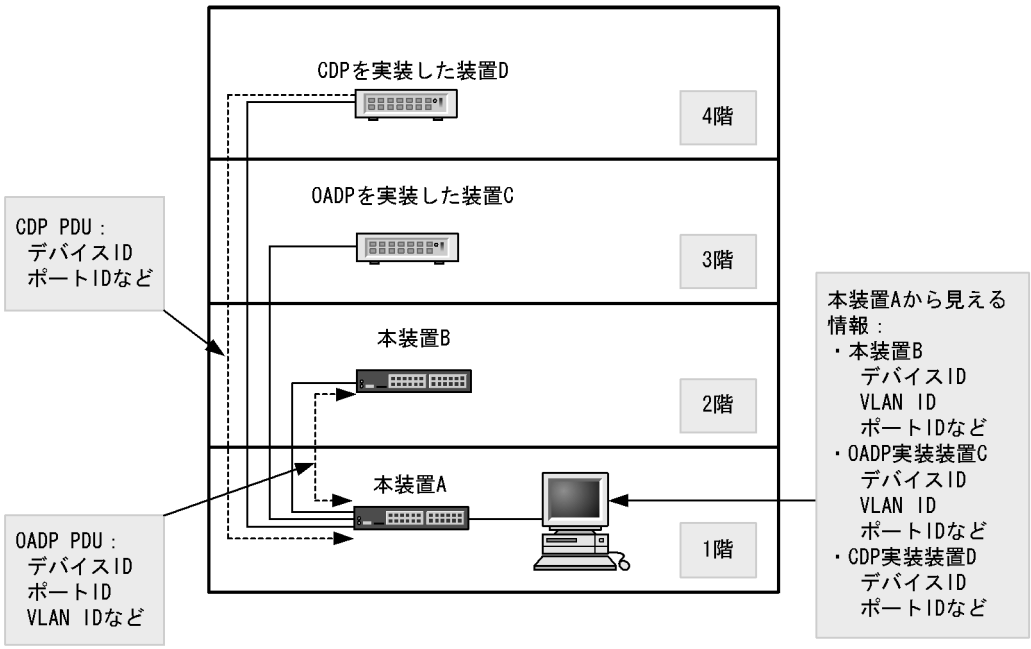
OADP 機能では，CDP（Cisco Discovery Protocol）を解釈できるため，CDP PDU を送信する隣接装置との接続構成も確認できます。ただし，本装置は CDP PDU を送信しません。CDP とは，Cisco Systems 社製装置のレイヤ 2 レベルで動作する隣接装置検出プロトコルです。

(3) OADP の適用例

OADP 機能を使用することで，隣接装置と接続している各ポートに対して自装置に関する情報および該当ポートに関する情報を送信します。自装置やポートに関する情報としては，デバイス ID，ポート ID，IP アドレス，VLAN ID などがあります。隣接装置から送られてきた情報を該当ポートで受信することで，自装置と隣接装置間の接続状態を把握できるようになります。

OADP の適用例を次の図に示します。この例では，同一ビル内の各階に設置された装置間の接続状態を，1 階に設置した本装置 A から把握することが可能となります。

図 25-1 OADP の適用例



25.1.2 サポート仕様

(1) OADP のサポート仕様

OADP でサポートする項目と仕様を次の表に示します。

表 25-1 OADP でサポートする項目・仕様

項目		内容
適用レイヤ	レイヤ 2	○
	レイヤ 3	×
OADP PDU 送受信単位		物理ポートまたはリンクアグリゲーション
リセット機能		○
OADP PDU 送信間隔		5 ～ 254 秒の範囲で 1 秒単位
OADP PDU 情報保有時間		10 ～ 255 秒の範囲で 1 秒単位
CDP 受信機能		○

（凡例） ○：サポート　×：未サポート

(2) OADP で使用する情報

OADP PDU で使用する情報を次の表に示します。

表 25-2 OADP でサポートする情報

項番	名称	説明
1	Device ID	装置を一意に識別する識別子
2	Address	OADP PDU を送信するインタフェースに関連するアドレス，およびループバックインタフェースのアドレス

項番	名称	説明
3	Port ID	OADP PDU を送信するポートの識別子
4	Capabilities	装置の機能
5	Version	ソフトウェアバージョン
6	Platform	プラットフォーム
7	Duplex	OADP PDU を送信するポートの Duplex 情報
8	ifIndex	OADP PDU を送信するポートの ifIndex
9	ifSpeed	OADP PDU を送信するポートの ifSpeed
10	VLAN ID	OADP PDU を送信するポートの VLAN ID
11	ifHighSpeed	OADP PDU を送信するポートの ifHighSpeed

受信する CDP PDU で使用される可能性のある情報を次の表に示します。項番 1 ～ 7 は OADP PDU と共通です。

表 25-3　CDP でサポートする情報

項番	名称	説明
1	Device ID	装置を一意に識別する識別子
2	Address	CDP PDU を送信するポートに関連するアドレス
3	Port ID	CDP PDU を送信するポートの識別子
4	Capabilities	装置の機能
5	Version	ソフトウェアバージョン
6	Platform	プラットフォーム
7	Duplex	CDP PDU を送信するポートの Duplex 情報

25.1.3　OADP 使用時の注意事項

(1) この機能を設定した装置間にこの機能をサポートしない別装置を接続した場合

次に示す構成とした場合，隣接装置との接続状態を正確に把握しにくい状態になります。

- スイッチを経由して接続した場合，スイッチは OADP の配布情報を中継します。そのため，直接接続していない装置間で隣接情報として配布情報を受信できるので，直接接続されている装置間の情報と区別が付かなくなります。
- ルータを経由して接続した場合，OADP の配布情報はルータで廃棄されるため OADP 機能を設定した装置間では受信できません。

(2) 隣接装置の最大数について

装置当たり最大 100 の隣接装置情報を収容できます。最大数を超えた場合，受信した配布情報は廃棄されます。受信済みの隣接装置情報がタイムアウトで削除される時間を確保するために廃棄状態は一定時間継続されます。時間は，最大収容数の閾値以上になった隣接装置情報の保持時間と同じです。

(3) OADP を使用するポートの VLAN について

OADP はポートに設定されている VLAN 上で OADP PDU を送受信します。VLAN を無効（state suspend コマンド）に設定するとその VLAN では OADP は動作しません。

(4) CDP を実装した装置と接続した場合について

トランクポートで CDP を実装した装置と接続した場合は，そのポートのネイティブ VLAN を無効（state suspend コマンド）にしないでください。無効に設定した場合，CDP PDU は本装置で廃棄されます。

(5) CDP を実装した装置間にあった L2 スイッチと本装置とを交換した場合について

CDP を実装した装置の間にあった（CDP を透過する）L2 スイッチを本装置に置き換えた場合に，本装置で CDP 受信機能を設定（oadp cdp-listener コマンド）すると，本装置が CDP PDU を受信して透過しなくなるため，CDP を実装した装置同士がお互いを認識できなくなります。CDP 受信機能を設定（oadp cdp-listener コマンド）しなければ，本装置は CDP PDU を受信しないで透過するので，装置を置き換える前と同様に CDP を実装した装置同士がお互いを認識できます。

(6) CFM との共存について

CFM とは同時に使用できません。

25.2 コンフィグレーション

25.2.1 コンフィグレーションコマンド一覧

OADP のコンフィグレーションコマンド一覧を次の表に示します。

表 25-4 コンフィグレーションコマンド一覧

コマンド名	説明
oadp cdp-listener	CDP 受信機能を有効にします。
oadp enable	ポートおよびリンクアグリゲーションで OADP 機能を有効にします。
oadp hold-time	本装置が送信する OADP フレームに対して隣接装置が保持する時間を指定します。
oadp ignore-vlan	指定した VLAN ID から受信する OADP フレームを無視する場合に指定します。
oadp interval-time	本装置が送信する OADP フレームの送信間隔を指定します。
oadp run	装置全体で OADP 機能を有効にします。

25.2.2 OADP の設定

(1) OADP 機能の設定

[設定のポイント]

OADP 機能のコンフィグレーションは装置全体で機能を有効にする設定と，実際に運用するポートで有効にする設定が必要です。

OADP を使用したいポートがリンクアグリゲーションを構成している場合は，ポートチャネルインタフェースに対して設定します。

ここでは，gigabitethernet 0/1 において OADP 機能を運用させます。

[コマンドによる設定]

1. **(config)# oadp run**
   装置全体で OADP 機能を有効にします。

2. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。

3. **(config-if)# oadp enable**
   ポート 0/1 で OADP 機能の動作を開始します。

[注意事項]

OADP は，設定したポートで有効な VLAN 上で動作します。suspend に設定されている VLAN では OADP は動作しません。

(2) OADP フレームの送信間隔，保持時間の設定

[設定のポイント]

OADP フレームの送信間隔を変更すると，装置の情報の変更が反映される時間を調整できます。送信間隔を短くすると変更が早く反映される一方で，自装置，隣接装置の負荷が高まる場合があります。

送信間隔を長くすると負荷は低くなりますが変更の反映が遅くなります。通常，本設定は変更する必要はありません。

[コマンドによる設定]

1. **(config)# oadp interval-time 60**
   OADP フレームの送信間隔を 60 秒に設定します。

2. **(config)# oadp hold-time 180**
   本装置が送信した情報を隣接装置が保持する時間を 180 秒に設定します。

(3) CDP 受信機能の設定

[設定のポイント]

CDP 受信機能を有効にすると，OADP が動作しているすべてのポートで CDP 受信機能が動作します。
ここでは，gigabitethernet 0/1 において CDP 受信機能を運用させます。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   ポート 0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# oadp enable**
   ポート 0/1 で OADP 機能を有効にします。

3. **(config-if)# exit**
   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から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)# oadp cdp-listener**
   CDP 受信機能を有効にします。OADP が動作しているポートで CDP 受信機能が動作します。

(4) OADP フレームを無視する VLAN の設定

[設定のポイント]

OADP は，トランクポートでは VLAN Tag を使用して 1 ポートに複数の OADP フレームを送受信します。トランクポートに所属している VLAN 数が増えると隣接装置情報も増加し，装置への負荷が増加します。受信した OADP フレームを無視する VLAN を設定することで装置への負荷を抑えられます。

[コマンドによる設定]

1. **(config)# oadp ignore-vlan 10-20**
   VLAN10 ～ 20 で受信した OADP フレームを無視します。

25.3 オペレーション

25.3.1 運用コマンド一覧

OADP の運用コマンド一覧を次の表に示します。

表 25-5 運用コマンド一覧

コマンド名	説明
show oadp	OADP/CDP の設定情報および隣接装置情報を表示します。
show oadp statistics	OADP/CDP 統計情報を表示します。
clear oadp	OADP/CDP の隣接情報をクリアします。
clear oadp statistics	OADP/CDP の統計情報をクリアします。
restart oadp	OADP プログラムを再起動します。
dump protocols oadp	OADP プログラムで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

25.3.2 OADP 情報の表示

OADP 情報の表示は，運用コマンド show oadp で行います。show oadp コマンドは，OADP の設定情報とポートごとの簡易的な情報を示します。show oadp detail コマンドは，隣接装置の詳細な情報を表示します。

図 25-2 show oadp コマンドの実行結果

```
> show oadp
Date 2005/11/09 19:50:20 UTC
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 0/1-5,16,20
              CH 10

Total Neighbor Counts=2
Local    VID Holdtime Remote   VID Device ID      Capability Platform
0/1        0       35 0/8        0 OADP-2         RS         AX3630S-24T2X
0/16       0        9 0/1        0 OADP-3         S          AX2430S-48T

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
>
```

図 25-3　show oadp detail コマンドの実行結果

```
> show oadp detail
Date 2005/11/09 19:55:52 UTC
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
Interval Time: 60   Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 0/1-5,16,20

Total Neighbor Counts=2
------------------------------------------------------
Port: 0/1   VLAN ID: 0
Holdtime      : 6(sec)
Port ID       : 0/8   VLAN ID(TLV): 0
Device ID     : OADP-2
Capabilities  : Router, Switch
Platform      : AX3630S-24T2X
Entry address(es):
    IP address  : 192.16.170.87
    IPv6 address: fe80::200:4cff:fe71:5d1c
IfSpeed       : 1G   Duplex    : FULL
Version      : ALAXALA AX3630S AX-3630S-24T2X [AX3630S-24T2X] Switching software
Ver. 10.0 [OS-L3L]
------------------------------------------------------
Port: 0/16   VLAN ID: 0
Holdtime      : 10(sec)
Port ID       : 0/1   VLAN ID(TLV): 0
Device ID     : OADP-3
Capabilities  : Switch
Platform      : AX2430S-48T
Entry address(es):
    IP address  : 192.16.170.100
IfSpeed       : 1G   Duplex    : FULL
Version       : ALAXALA AX2430S AX-2430S-48T [AX2430S-48T] Switching software
Ver. 10.0 [OS-L2]
------------------------------------------------------
>
```

26 ポートミラーリング

ポートミラーリングは，送受信するフレームのコピーを指定した物理ポートへ送信する機能です。この章では，ポートミラーリングの解説と操作方法について説明します。

26.1 解説

26.1.1 ポートミラーリングの概要

ポートミラーリングは，送受信するフレームのコピーを指定した物理ポートへ送信する機能です。フレームをコピーすることを**ミラーリング**と呼びます。この機能を利用して，ミラーリングしたフレームをアナライザなどで受信することによって，トラフィックの監視や解析を行えます。

受信フレームおよび送信フレームに対するミラーリングのそれぞれの動作を次の図に示します。

図 26-1 受信フレームのミラーリング

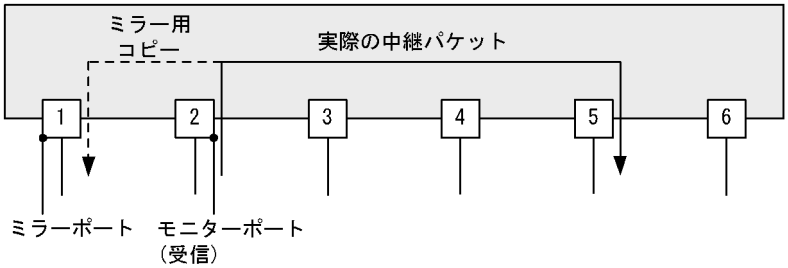
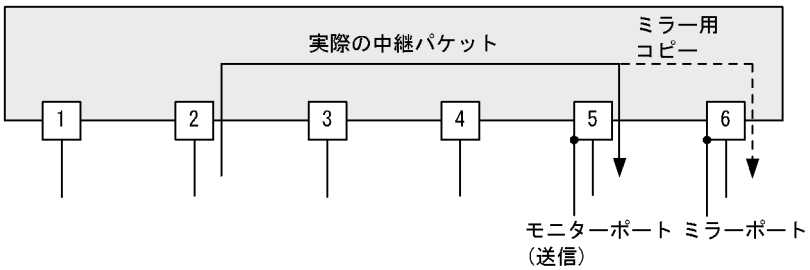


図 26-2 送信フレームのミラーリング



これらの図で示すとおり，トラフィックを監視する物理ポートを**モニターポート**と呼び，ミラーリングしたフレームの送信先となる物理ポートを**ミラーポート**と呼びます。

ミラーポートからはミラーリングされたフレームだけ送信されます。それ以外の自発，自宛，中継フレームは廃棄されます。ただし，制御フレームが送信される設定をした場合，設定された制御フレームは送信されます。なお，ミラーリングしたフレームは，TTL（IPv4）またはホップリミット（IPv6）を減算しないで送信されます。

また，モニターポートとミラーポートは「多対一」の設定ができ，複数のモニターポートから受信したフレームのコピーを，一つのミラーポートへ送信できます。ただし，モニターポートでコピーしたフレームを複数のミラーポートへ送信することはできません。

ポートミラーリングに関する運用コマンドはありません。ミラーポートに接続したアナライザで，フレームがミラーリングされていることを確認してください。

26.1.2 ポートミラーリングの注意事項

(1) 他機能との共存

- モニターポートでは，ほかの機能は制限なく動作します。
- ミラーポートでは，VLAN 機能およびレイヤ 3 通信機能が使用できません。VLAN 機能を前提とする

スパニングツリー，Ring Protocol，IGMP snooping/MLD snooping などの機能や，レイヤ 3 通信機能を前提とする SNMP，DHCP などの機能も使用できません。

- ミラーポートに制御フレームが送信される機能を設定すると，コピーされたフレームのほかに設定された制御フレームが送信されます。
- DHCP snooping を有効にした場合，本装置が送信するすべての DHCP パケットはミラーリングされません。また，ダイナミック ARP 検査も有効にした場合，本装置が送信するすべての ARP パケットもミラーリングされません。

(2) ポートミラーリング使用時の注意事項

- ポートミラーリングでコピーしたフレームは，ミラーポートの回線帯域を超えて出力することはできません。
- 受信したフレームの FCS が不正な場合，該当フレームはミラーリングされません。
- モニターポートに対して，フィルタ /QoS 制御やストームコントロールを設定できますが，ポートミラーリング機能には影響しません。
- 送信フレームのミラーリングでは，ハードウェアで中継するフレームだけをミラーリングします。ソフトウェアで送信するフレーム（自発，IP オプション付きパケットなど）はミラーリングしません。受信フレームのミラーリングでは，自宛フレームや IP オプション付きパケットなどを含めた，すべての受信フレームをミラーリングします。
- 送信フレームのミラーリングでは，1 セッションだけ設定できます。
- 送信フレームのミラーリングで複数モニターポートを設定し，そのすべてまたは一部のポートにフレームをフラッディングする場合，ミラーリングするフレームは次のようになります。
  - 該当するポートが 0/1 ～ 0/24 および 0/49，0/50 と，0/25 ～ 0/48 にわたっている場合，2 個のフレームがミラーリングされます。
  - 上記以外の場合，1 個のフレームがミラーリングされます。
- 送信フレームのミラーリングでは，Untagged フレームを送信する場合でも，送信フレームの VLAN の Tag を持つ Tagged フレームがミラーリングされます。
- 送信フレームのミラーリングでは，送信ポートに Tag 変換機能が設定されていても，LAN 上で使用する VLAN Tag ではなく，送信フレームの VLAN の Tag を持つ Tagged フレームがミラーリングされます。
- 受信フレームのミラーリングで，次に示す条件がすべて一致する場合，ミラーリングしたフレームの受信 VLAN Tag の前に，4095 またはネイティブ VLAN の VLAN Tag が余計に付くことがあります。
  - AX2430S-48T または AX2430S-48TD モデルを使用する。
  - モニターポートに Tag 変換機能を一つ以上設定している。
  - 受信したフレームの VLAN Tag を Tag 変換機能で設定していない（対象フレームは中継せずに廃棄されます。）。
  - モニターポートが 1 ～ 24 のどれかでミラーポートが 25 ～ 48 のどれか，またはモニターポートが 25 ～ 48 のどれかかつミラーポートが 1 ～ 24 のどれかでポートミラーリングを設定している。

26.2 コンフィグレーション

26.2.1 コンフィグレーションコマンド一覧

ポートミラーリングのコンフィグレーションコマンド一覧を次の表に示します。

表 26-1 コンフィグレーションコマンド一覧

コマンド名	説明
monitor session	ポートミラーリングを設定します。

26.2.2 ポートミラーリングの設定

ポートミラーリングのコンフィグレーションでは，モニターポートとミラーポートの組み合わせをモニターセッションとして設定します。本装置では最大 4 組のモニターセッションを設定できます。

組み合わせごとに 1 から 4 のセッション番号を使用します。設定したモニターセッションを削除する場合は，設定時のセッション番号を指定して削除します。設定済みのセッション番号を指定すると，モニターセッションの設定内容は変更されて，以前のモニターセッションの情報は無効になります。

モニターポートには，通信で使用するポートを指定します。ミラーポートには，トラフィックの監視や解析などのために，アナライザなどを接続するポートを指定します。ミラーポートではポートミラーリング以外の通信はできません。

送信フレームのミラーリングおよび送受信フレームのミラーリングはセッション番号 1 のモニターセッションにだけ設定できます。

(1) 受信フレームのミラーリング

[設定のポイント]

設定できるインタフェースはイーサネットインタフェースです。リンクアグリゲーションで使用している場合も，単独のイーサネットインタフェースを指定します。また，ミラーポートは vlan などを設定していないポートに設定します。

[コマンドによる設定]

1. **(config)# monitor session 2 source interface gigabitethernet 0/1 rx destination interface gigabitethernet 0/5**
   アナライザをポート 0/5 に接続し，1G ビットイーサネットインタフェース 0/1 で受信するフレームをミラーリングすることを設定します。セッション番号は 2 を使用します。

(2) 送信フレームのミラーリング

[設定のポイント]

設定できるインタフェースはイーサネットインタフェースです。リンクアグリゲーションで使用している場合も，単独のイーサネットインタフェースを指定します。また，ミラーポートは vlan などを設定していないポートに設定します。セッション番号は 1 でなければなりません。

[コマンドによる設定]

1. **(config)# monitor session 1 source interface gigabitethernet 0/2 tx destination interface gigabitethernet 0/6**

アナライザをポート 0/6 に接続し，1G ビットイーサネットインタフェース 0/2 で送信するフレームをミラーリングすることを設定します。セッション番号は 1 を使用します。

(3) 送受信フレームのミラーリング

[設定のポイント]

設定できるインタフェースはイーサネットインタフェースです。リンクアグリゲーションで使用している場合も，単独のイーサネットインタフェースを指定します。また，ミラーポートは vlan などを設定していないポートに設定します。セッション番号は 1 でなければなりません。

[コマンドによる設定]

1. **(config)# monitor session 1 source interface gigabitethernet 0/3 both destination interface gigabitethernet 0/11**
   アナライザをポート 0/11 に接続し，1G ビットイーサネットインタフェース 0/3 で送受信するフレームをミラーリングすることを設定します。セッション番号は 1 を使用します。

(4) 複数モニターポートのミラーリング

[設定のポイント]

複数のモニターポートをリスト形式で設定できます。設定済みのリストにポートを追加することや，削除することもできます。

[コマンドによる設定]

1. **(config)# monitor session 1 source interface gigabitethernet 0/1-23,tengigabitethernet 0/25 both destination interface gigabitethernet 0/24**
   アナライザをポート 0/24 に接続し，1G ビットイーサネットインタフェース 0/1 から 0/23 および 10G ビットイーサネットインタフェース 0/25 で送受信するフレームをミラーリングすることを設定します。セッション番号は 1 を使用します。

付録

付録 A　準拠規格

付録 A　準拠規格

付録 A.1　Diff-serv

表 A-1　Diff-serv の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2474(1998 年 12 月)	Definition of the Differentiated Services Field(DS Field) in the IPv4 and IPv6 Headers
RFC2475(1998 年 12 月)	An Architecture for Differentiated Services
RFC2597(1999 年 6 月)	Assured Forwarding PHB Group
RFC3246(2002 年 3 月)	An Expedited Forwarding PHB (Per-Hop Behavior)
RFC3260(2002 年 4 月)	New Terminology and Clarifications for Diffserv

付録 A.2　IEEE802.1X

表 A-2　IEEE802.1X の準拠規格および勧告

規格番号 (発行年月)	規格名
IEEE802.1X(2001 年 6 月)	Port-Based Network Access Control
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service (RADIUS)
RFC2866(2000 年 6 月)	RADIUS Accounting
RFC2868(2000 年 6 月)	RADIUS Attributes for Tunnel Protocol Support
RFC2869(2000 年 6 月)	RADIUS Extensions
RFC3162(2001 年 8 月)	RADIUS and IPv6
RFC3579(2003 年 9 月)	RADIUS Support For Extensible Authentication Protocol (EAP)
RFC3580(2003 年 9 月)	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
RFC3748(2004 年 6 月)	Extensible Authentication Protocol (EAP)

付録 A.3　Web 認証

表 A-3　Web 認証の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service (RADIUS)
RFC2866(2000 年 6 月)	RADIUS Accounting
RFC3162(2001 年 8 月)	RADIUS and IPv6

付録 A.4　MAC 認証

表 A-4　MAC 認証の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service (RADIUS)
RFC2866(2000 年 6 月)	RADIUS Accounting
RFC3162(2001 年 8 月)	RADIUS and IPv6

付録 A.5　DHCP snooping

表 A-5　DHCP snooping の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2131(1997 年 3 月)	Dynamic Host Configuration Protocol

付録 A.6　IEEE802.3ah/UDLD

表 A-6　IEEE802.3ah/UDLD の準拠規格および勧告

規格番号 (発行年月)	規格名
IEEE802.3ah(2004 年 9 月)	Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks

付録 A.7　CFM

表 A-7　CFM の準拠規格および勧告

規格番号 (発行年月)	規格名
IEEE802.1ag-2007(2007 年 12 月)	Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management

付録 A.8　SNMP

表 A-8　SNMP の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1155(1990 年 5 月)	Structure and Identification of Management Information for TCP/IP-based Internets
RFC1157(1990 年 5 月)	A Simple Network Management Protocol (SNMP)
RFC1901(1996 年 1 月)	Introduction to Community-based SNMPv2
RFC1902(1996 年 1 月)	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1903(1996 年 1 月)	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1904(1996 年 1 月)	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)

規格番号 (発行年月)	規格名
RFC1905(1996 年 1 月)	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1906(1996 年 1 月)	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1907(1996 年 1 月)	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1908(1996 年 1 月)	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC2578(1999 年 4 月)	Structure of Management Information Version 2 (SMIv2)
RFC2579(1999 年 4 月)	Textual Conventions for SMIv2
RFC2580(1999 年 4 月)	Conformance Statements for SMIv2
RFC3410(2002 年 12 月)	Introduction and Applicability Statements for Internet Standard Management Framework
RFC3411(2002 年 12 月)	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC3412(2002 年 12 月)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC3413(2002 年 12 月)	Simple Network Management Protocol (SNMP) Applications
RFC3414(2002 年 12 月)	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC3415(2002 年 12 月)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC3416(2002 年 12 月)	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC3417(2002 年 12 月)	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC3584(2003 年 8 月)	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework

表 A-9　MIB の準拠規格および勧告

規格番号 (発行年月)	規格名
IEEE8023-LAG-MIB(2000 年 3 月)	Aggregation of Multiple Link Segments
IEEE8021-PAE-MIB(2001 年 6 月)	Port-Based Network Access Control
IEEE8021-CFM-MIB(2007 年 12 月)	Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management
RFC1158(1990 年 5 月)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC1213(1991 年 3 月)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC1493(1993 年 6 月)	Definitions of Managed Objects for Bridges
RFC1643(1994 年 7 月)	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC1757(1995 年 2 月)	Remote Network Monitoring Management Information Base
RFC2233(1997 年 11 月)	The Interfaces Group MIB using SMIv2
RFC2452(1998 年 12 月)	IP Version 6 Management Information Base for the Transmission Control Protocol

規格番号 (発行年月)	規格名
RFC2454(1998 年 12 月)	IP Version 6 Management Information Base for the User Datagram Protocol
RFC2465(1998 年 12 月)	Management Information Base for IP Version 6: Textual Conventions and General Group
RFC2466(1998 年 12 月)	Management Information Base for IP Version 6: ICMPv6 Group
RFC2674(1999 年 8 月)	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions
RFC3411(2002 年 12 月)	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC3412(2002 年 12 月)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC3413(2002 年 12 月)	Simple Network Management Protocol (SNMP) Applications
RFC3414(2002 年 12 月)	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC3415(2002 年 12 月)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC3418(2002 年 12 月)	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

付録 A.9　SYSLOG

表 A-10　SYSLOG の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC3164(2001 年 8 月)	The BSD syslog Protocol

付録 A.10　sFlow

表 A-11　sFlow の準拠規格および勧告

規格番号（発行年月）	規格名
RFC3176(2001 年 9 月)	InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks

付録 A.11　LLDP

表 A-12　LLDP の準拠規格および勧告

規格番号 (発行年月)	規格名
IEEE802.1AB/D6.0(2003 年 10 月)	Draft Standard for Local and Metropolitan Networks: Station and Media Access Control - Connectivity Discovery

索引

O

P

Q

R

S

T

U

V

W

あ

い

え

き

こ

さ

し

す

そ

た

と

な

に

ね

は

ひ

ふ

ほ

ま

み

も

ゆ

れ

ろ

わ